UNIVERSIDADE DE BRASÍLIA

FACULDADE DE DIREITO

ANA BEATRIZ GONÇALVES FELIZ

TESTANDO O RECONHECIMENTO FACIAL NAS RUAS:

Uma breve análise dos custos e riscos de seu uso na Segurança Pública do Uruguai e Brasil

Brasília-DF

2025

ANA BEATRIZ GONÇALVES FELIZ

TESTANDO O RECONHECIMENTO FACIAL NAS RUAS:

Uma breve análise dos custos e riscos de seu uso na Segurança Pública do Uruguai e Brasil

Trabalho de Conclusão de Curso apresentado ao Programa de Graduação em Direito da Universidade de Brasília (UnB) como requisito parcial para a obtenção do grau de Bacharel em Direito.

Orientadora: Prof.ª Dr.ª Fernanda de Carvalho Lage.

Brasília-DF

2025

ANA BEATRIZ GONÇALVES FELIZ

TESTANDO O RECONHECIMENTO FACIAL NAS RUAS:
Uma breve análise dos custos e riscos de seu uso na Segurança Pública do Uruguai e Brasil

Trabalho de Conclusão de Curso apresentado ao Programa de Graduação em Direito da Universidade de Brasília (UnB) como requisito parcial para a obtenção do grau de Bacharel em Direito.

Orientadora: Prof.ª Dr.ª Fernanda de Carvalho Lage.

Brasília, 14 de fevereiro de 2025

BANCA EXAMINADORA

Prof.ª Dr.ª Fernanda de Carvalho Lage

Prof. Dr. Evandro C. Piza Duarte

Doutorando Pedro Diogo Carvalho Monteiro

Brasília-DF

2025

AGRADECIMENTOS

Inicialmente, deixo uma ênfase para a dificuldade de resumir toda a gratidão acumulada em torno desses últimos cinco anos atípicos. Foram várias as figuras que, nos momentos de desânimo e entusiasmo, vieram compartilhar suas histórias e trajetórias comigo. Sou grata por essas histórias de vida, casos de trabalho e reclamações, isso alegrou meus dias enclausurados num quarto por conta da pandemia. Em tempos pandêmicos, a experiência universitária poderia ter se resumido às aulas no Teams. Esse seria o esperado. Acontece que a Providência sempre dá um jeito de nos levar por caminhos complicados e interessantes.

Vejamos, minha trajetória poderia ter se resumido às aulas e estágio. Mas não foi bem assim. Logo nos primeiros semestres, entrei em contato com a tal Criminologia Crítica e nunca mais larguei as aulas. No antes e depois da minha vida universitária, posso apontar essas aulas como um "divisor de águas". Sou grata por essa oportunidade proporcionada pelo Prof. Evandro, bem como tantas outras. As aulas nas turmas do programa de pós passaram a ser um alento em meio às semanas conturbadas no estágio.

E, junto das aulas de Criminologia, elogio as de Direito do Trabalho, individual ou coletivo, o entusiasmo das professoras Gabriela e Erica resgataram aquele meu sonho de criança de debater os casos trabalhistas. Sim, parece estranho, mas passei parte da minha infância escutando as histórias que meu pai me contava da faculdade de direito. Em parte, escolhi o curso por conta dessas histórias, elas eram tão absurdas e revoltantes que despertaram um senso de "preciso fazer algo" ou "isso está muito errado". Não que eu tenha feito muito com o meu aprendizado, ainda mais quando me deparei com as histórias igualmente revoltantes com que trabalhei na Defensoria.

E por falar em Defensoria, deixo aqui registrada a minha sincera gratidão à Dra. Ana Paula, que com muita paciência acreditou no meu potencial para desenvolver as complicadas peças trabalhistas. Até hoje estou em busca desse potencial, mas matemática nunca foi meu forte. Inclusive, destaco aqui meu sincero obrigada ao meu namorado, que, com uma paciência admirável, leu este trabalho e corrigiu as partes referentes ao funcionamento do reconhecimento facial.

Enfim, agradeço a Deus e à Nossa Senhora, que com muita paciência me guiaram nesses anos e permitiram que eu tenha chegado bem, sã e com disposição, neste fim de curso. Agradeço aos meus familiares, especialmente à minha mãe e ao meu pai, que, com tanto carinho, me apoiaram ao longo desses anos. Deixo aqui minha sincera gratidão às minhas amigas e colegas de curso. A todas e todos, direciono o meu sincero obrigada!

“Tinha as forças comuns, mas uma grande coragem. Ao lado da força, que é física, tinha a energia, que é moral. Devia praticar ali um ato tremendo. Galgar, suspenso aquele fio, o intervalo de duas Douvres; tal era a questão. São frequentes nos atos de dedicação ou de dever esses pontos de interrogação que parecem postos pela morte. Farás isto?” (Hugo, Victor, 1971, p.236).

RESUMO

Apontado como a "inovação" nos sistemas de vigilância e monitoramento das ruas, o reconhecimento de imagens é a nova aposta para a "modernização" do enfrentamento e combate ao crime organizado. Seja nas arquibancadas ou nas ruas, o reconhecimento de imagens pode ser útil para flagrar torcedores violentos e foragidos. Contudo, dentre os elementos do reconhecimento de imagens, um deles tem sido palco para polêmicas quanto ao seu uso e funcionamento: o reconhecimento facial. Conhecido como uma "caixa preta" de números e informações indecifráveis para os seus próprios programadores, o FRT é percebido com desconfiança pela sociedade civil, ao passo que o Estado o aplaude. As estatísticas de êxito guardam a dúvida quanto aos critérios utilizados e à "margem de erro", ao passo que as próprias "falhas" dos algoritmos passam a ser questionáveis. Na confecção do reconhecimento facial, vários de seus componentes básicos podem ser tocados por vieses subjetivos, ao ponto de o resultado final ter a sua neutralidade questionada. Nesse raciocínio, o presente trabalho desenvolve-se com vistas a compreender o cenário em que as tecnologias de reconhecimento de imagem, em especial o reconhecimento facial, são inseridas no cenário de consumo da vigilância pública. Para atingir esse fim, o estudo pautou-se nos conceitos de "capitalismo de vigilância" e "tecnosolucionismo", desenvolvidos por Zuboff e Ribeiro, respectivamente. Posteriormente, prosseguiu-se para a pesquisa quanto ao funcionamento da tecnologia de reconhecimento facial, seus problemas operacionais e formas de incorporação de vieses raciais e de gênero: nessa etapa, buscou-se suporte teórico nos estudos dos matemáticos Joy Buolamwini e Diogo Brandão. Após a análise desses conceitos iniciais, tais premissas são levadas ao campo fático. Para isso, foram selecionados o Uruguai e o Ceará para proporcionar o estudo das influências que definiram a implementação da FRT e os usos dados à tecnologia de videomonitoramento. Nesse sentido, foram realizados dois estudos de casos: o primeiro referente à contratação de tecnologias de monitoramento por parte do *Ministerio del Interior* e o segundo abarcando as contratações realizadas pelo Governo do Estado do Ceará. A metodologia utilizada conta com revisão de bibliografia especializada, mapeamento de notícias, buscas junto aos sistemas de licitações e mapeamento das decisões presentes no banco de jurisprudência uruguaia. Por fim, foi feita uma análise do arcabouço normativo que ampara o uso da tecnologia de reconhecimento facial no Uruguai e no Ceará. No decurso da pesquisa, evidenciou-se a ausência de processos ajuizados no Tribunal de Justiça do Ceará que digam respeito ao uso das tecnologias de videomonitoramento na segurança pública, razão pela qual se optou por pormenorizar as formas de regulação da FRT no Estado.

Palavras-Chave: Reconhecimento Facial, Segurança Pública, Dados Pessoais, Transparência.

RESUMEN

Considerado como la "innovación" en los sistemas de vigilancia y monitoreo de calles, el reconocimiento de imágenes es la nueva apuesta para la "modernización" del enfrentamiento y combate al crimen organizado. Ya sea en las gradas o en las calles, el reconocimiento de imágenes puede resultar útil para atrapar a aficionados violentos y fugitivos. Sin embargo, entre los elementos del reconocimiento de imágenes, uno de ellos ha sido escenario de polémica respecto a su uso y funcionamiento: el reconocimiento facial. Conocido como una "caja negra" de números e información indescifrable para sus propios programadores, el FRT es percibido con recelo por la sociedad civil, mientras el Estado lo aplaude. Las estadísticas de éxito plantean dudas sobre los criterios utilizados y el "margen de error", mientras que los "defectos" de los propios algoritmos se vuelven cuestionables. A la hora de crear el reconocimiento facial, varios de sus componentes básicos pueden verse afectados por sesgos subjetivos, hasta el punto de que el resultado final tiene en duda su neutralidad. Siguiendo este razonamiento, el presente trabajo se desarrolla con miras a comprender el escenario en el que las tecnologías de reconocimiento de imágenes, especialmente el reconocimiento facial, se insertan en el escenario de consumo de la vigilancia pública. Para lograr este fin, el estudio se basó en los conceptos de "capitalismo de vigilancia" y "tecnosolucionismo", desarrollados por Zuboff y Ribeiro, respectivamente. Posteriormente, continuaron las investigaciones sobre el funcionamiento de la tecnología de reconocimiento facial, sus problemas operativos y las formas de incorporar sesgos raciales y de género: en esta etapa, se buscó apoyo teórico en los estudios de los matemáticos Joy Buolamwini y Diogo Brandão. Luego de analizar estos conceptos iniciales, tales premisas se llevan al campo fáctico, para ello se seleccionó a Uruguay y Ceará para brindar el estudio de las influencias que definieron la implementación de FRT y los usos dados a la tecnología de video monitoreo. En este sentido, se realizaron dos estudios de caso: el primero referido a la contratación de tecnologías de monitoreo por parte del Ministerio del Interior y el segundo abarcando los contratos realizados por el Gobierno del Estado de Ceará. La metodología utilizada incluye una revisión de bibliografía especializada, mapeo de noticias, búsquedas de sistemas de licitación y mapeo de decisiones presentes en la base de datos de jurisprudencia uruguaya. Finalmente, se realizó un análisis del marco regulatorio que sustenta el uso de la tecnología de reconocimiento facial en Uruguay y Ceará. Durante la investigación, quedó claro que no hubo casos presentados ante el Tribunal de Justicia de Ceará que se refieran al uso de tecnologías de videovigilancia en la seguridad pública, por lo que se decidió detallar las formas de regulación del FRT en el Estado.

Palabras clave: Reconocimiento Facial, Seguridad Pública, Datos Personales, Transparencia.

ABSTRACT

Touted as the “innovation” in street surveillance and monitoring systems, image recognition is the new bet for the “modernization” of confronting and combating organized crime. Whether in the stands or on the streets, image recognition can be useful in catching violent fans and fugitives. However, among the elements of image recognition, one of them has been the stage for controversy regarding its use and functioning: facial recognition. Known as a “black box” of numbers and information that is indecipherable to its own programmers, the FRT is perceived with suspicion by civil society, while the State applauds it. Success statistics raise doubts regarding the criteria used and the “margin of error”, while the “flaws” of the algorithms themselves become questionable. When creating facial recognition, several of its basic components can be affected by subjective biases, to the point that the final result has its neutrality questioned. Following this reasoning, the present work is developed with a view to understanding the scenario in which image recognition technologies, especially facial recognition, are inserted into the consumption scenario of public surveillance. To achieve this end, the study was based on the concepts of “surveillance capitalism” and “technosolutionism”, developed by Zuboff and Ribeiro, respectively.Subsequently, research continued into the functioning of facial recognition technology, its operational problems and ways of incorporating racial and gender biases: at this stage, theoretical support was sought in the studies of mathematicians Joy Buolamwini and Diogo Brandão. After analyzing these initial concepts, such premises are taken to the factual field, for this, Uruguay and Ceará were selected to provide the study of the influences that defined the implementation of FRT and the uses given to video monitoring technology. In this sense, two case studies were carried out: the first referring to the contracting of monitoring technologies by the Ministry of the Interior and the second covering the contracts carried out by the Government of the State of Ceará. The methodology used includes a review of specialized bibliography, mapping of news, searches of bidding systems and mapping of decisions present in the Uruguayan jurisprudence database.Finally, an analysis was made of the regulatory framework that supports the use of facial recognition technology in Uruguay and Ceará. During the research, it became clear that there were no cases filed at the Court of Justice of Ceará that concern the use of video monitoring technologies in public security, which is why it was decided to detail the forms of regulation of FRT in the State.

Keywords: Facial Recognition, Public Security, Personal Data, Transparency.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

AL: América Latina;

ARCE: Agencia Reguladora de Compras Estatales;

AUF: Asociación Uruguaya de Fútbol;

COR: Centro de Operações Rio;

CVLI: Crimes Violentos Letais Intencionais;

ETICE: Empresa de Tecnologia e Informação do Estado do Ceará;

FRT: Facial Recognition Technology/Tecnologia de reconhecimento facial;

IA: Inteligência Artificial;

LGPD: Lei Geral de Proteção de Dados Pessoais;

LPDP: Ley de Proteccion de Datos Personales;

MI: Ministerio del Interior;

OCR: Optical Character Recognition/ Reconhecimento óptico de caracteres.

SUMÁRIO

1. INTRODUÇÃO

Ao deparar-se com o tema desta pesquisa, uma das primeiras impressões beira a sensação de que se trata de um tema futurístico e atrelado aos cenários distópicos imaginados por roteiristas, em que a tecnologia domina o mundo das coisas e as pessoas passam a ser guiadas por um complexo conjunto de números. Não é esse o tópico aqui abordado.

Também não se trata do cenário imaginado por Orwell (2009) em seu livro 1984. Sua trama destaca que as cidades estão cercadas por milhares de câmeras a serviço da figura ditatorial do *Big Brother*, que destinam ao monitoramento dos cidadãos e servem de material para a elaboração de fichas sobre os hábitos dos cidadãos.

A pesquisa diz respeito a uma tecnologia mais discreta e flexível. Despercebida e sem o controle monopolizado pela figura estatal. Mas sim, um mecanismo que é posto ao serviço da eficiência da cidade e, concomitantemente, utilizado como rede para apanhar as informações oferecidas pelos transeuntes e usuários. Trata-se de uma tecnologia de reconhecimento de imagens, uma ferramenta útil e inteligente, que, como desdobramento da Inteligência Artificial (IA), foi sendo introduzida aos poucos no cotidiano.

Nas palavras do ex-presidente da Google China e um dos principais executivos da Microsoft e Apple, Kai-Fu Lee (2019), os cenários futuristas que tratam da revolução completa da IA e sua inserção total na vida cotidiana estão longe e passam pelo cumprimento de etapas: as "ondas" da IA que são divididas em eixos como *internet*, negócios, percepção e IA autônoma. As primeiras duas fases já se encontram integradas com o mundo das coisas, em que nelas se observa que as máquinas já estão atuando como garimpadoras e consultoras. No início, informações como as curtidas, tempo de página e compras são transformadas em dados e devidamente "rotuladas". Posteriormente, a máquina utiliza essas etiquetas para aprender os hábitos e preferências dos consumidores e direcioná-los aos conteúdos selecionados (Lee, 2019). Uma ferramenta útil para o *marketing* e para empresas como o Google, que lucram ao catalogar as informações e leiloá-las para as empresas de publicidade (Lee, 2019). Quanto à terceira onda, essa merece especial destaque.

Lee (2019) também faz menção a uma etapa caracterizada pela superação da dificuldade em codificar os ambientes auditivos e visuais. Na onda da percepção, a IA é capaz de reconhecer os *pixels* de uma foto e atribuir significados à imagem e comandos de voz, ao ponto de tornar-se a conexão entre os "mundos *online* e *offline*", sincronizando-os (Lee, 2019). E para estabelecer esse elo entre o mundo dos fatos e o das redes, são essenciais ferramentas, como o Reconhecimento Facial (FRT) e o Reconhecimento Óptico de Caracteres (OCR).

Tais mecanismos fazem a leitura das imagens, sejam rostos ou placas de carro, e os tornam em dados legíveis para as máquinas. Todavia, não se trata apenas de leitura de dados, mas sim da interpretação e catalogação destes, em tempo real.

Essa "leitura dinâmica" feita pelas máquinas de reconhecimento dá-se através do uso de algoritmos para melhorar o seu desempenho, ferramentas destinadas a aprender mais e mais rápido. Compostos por padrões matemáticos que visam "generalizar dados" e utilizá-los para formar decisões, os algoritmos são modelos usados na predição de informações, que após o treinamento proporcionado por um vasto banco de dados, é continuamente ajustado para fazer previsões cada vez melhores (Brandão, 2023). Um exemplo prático é o uso de câmeras espalhadas pelas ruas, destinadas ao monitoramento dos espaços públicos.

Em cidades como o Rio de Janeiro, foi adotado o Centro de Operações Rio, em que se destacam: a combinação das informações das câmaras nas ruas com os dados provenientes das estações meteorológicas e serviços como Waze e Twitter; correlação dos dados compilados para proporcionar uma perspectiva integrada da cidade; projeção de diagnósticos de "normalidade", "atenção" e "crise" (Bruno, 2018). Nas cidades conectadas, as câmeras, mídias sociais e a *internet* fazem a captação dos dados que serão interpretados e ressignificados pelos algoritmos. Ademais, há outros usos de tais ferramentas nos espaços públicos e privados, como a coleta de dados no mundo *offline* visando gerar lucro.

Com câmeras espalhadas em locais estratégicos, como portas e laterais das vitrines externas das lojas, é possível coletar dados como a reação do transeunte, tempo de envolvimento do sujeito, sua faixa etária, gênero e rosto: dados esses que são coletados e ajudam a traçar o "perfil de consumo" de cada transeunte, ao ponto de servirem de base para a compreensão do público consumidor (Silva, 2023). Essa coleta de dados pode ocorrer tanto em espaços privados, como nas lojas, bem como nos espaços públicos, tais quais as ruas e estações de metrô. Um caso emblemático diz respeito ao Metrô de São Paulo.

Em sua linha 4 Amarela, havia painéis nas portas de entrada e saída das estações que, enquanto vinculavam propagandas publicitárias, captavam a reação dos passageiros por meio de suas câmeras: o objetivo da concessionária era a criação de um banco de dados, com o mapeamento das preferências de potenciais clientes, e negociá-lo a fim de aumentar a margem do lucro com a cessão dos espaços para a publicidade (Andrea; Silva; Gundim; 2022).

Não tardou para que tal iniciativa fosse questionada pelo Instituto de Defesa do Consumidor por meio da via judicial: no julgamento da ação, foi constatado que a concessionária captava e tratava as imagens dos usuários sem a autorização destes, situação que fere diretamente o direito à privacidade e autodeterminação dos dados pessoais, de modo que a concessionária foi condenada a pagar cem mil reais em danos morais coletivos e cessar o serviço de captura de imagens (Andrea; Silva; Gundim; 2022).

As situações apresentadas, seja da correlação dos dados capturados nas vias públicas ao uso destes para a elaboração de perfis dos transeuntes e potenciais consumidores, beiram a penumbra da zona limítrofe da coleta de dados no espaço público. Pois, ainda que o sujeito esteja na rua e não seja diretamente impactado pela captura e catalogação de seus dados, essa exposição excessiva pode implicar violação de seu direito à proteção de seus dados pessoais. Tais dados encontram amparo na Lei Geral de Proteção de Dados Pessoais (LGPD), cuja aplicação se dá no cenário de constantes inovações tecnológicas e demandas por soluções práticas. Trata-se, então, do conjunto de medidas para direcionar políticas públicas e padrões de boas práticas a serem seguidos, cujos parâmetros devem ser aplicados em qualquer situação (Silva, 2023), desde a segurança pública ao *marketing*.

Todavia, tal proteção tem tornado-se cada vez mais desafiada. Tornou-se complexo manter e garantir as dimensões do direito à privacidade, como:

a) A transparência do processamento de dados;
b) Explicação dos seus riscos;
c) Informar o usuário;
d) Tomar o seu consentimento;
e) Bem como corrigir as informações coletadas e cadastradas (Silva, 2023).

Tal dificuldade advém principalmente da necessidade de se conciliar os direitos dos usuários com a velocidade de coleta e propagação das informações, bem como com a pretensa necessidade e urgência de se modernizar os sistemas de vigilância dos espaços públicos.

Na atual conjectura, toda e qualquer informação coletada possui valor econômico. Nenhuma das “pegadas” e “rastros” deixados pelo usuário e transeunte são desperdiçadas. Dados como buscas, e-mails, localizações, reações, erros ortográficos, visualizações de páginas não são triviais e tampouco efémeros, pelo contrário, tais informações são capturadas, agregadas e vendidas (Zuboff; Bruno, 2018).

São processos unilaterais em que não há entrega ou reciprocidade entre quem coleta e quem tem os dados extraídos, é um procedimento que "toma" os dados pessoais do usuário sem qualquer diálogo ou negociação prévia (Zuboff; Bruno, 2018). Essa busca incessante pelo lucro advindo do leilão de informações é componente estrutural da lógica de acumulação do "capitalismo de vigilância": um projeto de extração de dados pautado na indiferença com os seus proprietários (Zuboff; Bruno, 2018).

Outro fator que desafia a garantia dos desdobramentos do direito à privacidade dos usuários e transeuntes consiste na cultura de pronta absorção das inovações tecnológicas em prol da segurança pública. É uma variação de "fetichismo" com idolatria das tecnologias de vigilância que se traduz na plena confiança de sua eficiência (Firmino; Bruno, 2018), cujo resultado consiste na defesa de sua aplicação à margem da LGPD. São estratégias de gestão e controle das ações no espaço urbano que objetivam a criação de "territórios securitizados" nos espaços públicos e privados: espaços que produzem a classificação social e espacial dos transeuntes, a fim de determinar padrões de "normalidade" e detectar os comportamentos desviantes (Firmino; Bruno, 2018). Trata-se de uma forma de controle discreta e flexível.

Ante o exposto, o presente trabalho tem como objetivo abordar o cenário da introdução da tecnologia de reconhecimento de imagens, em especial da FRT, na segurança pública uruguaia e brasileira. Para atender a esse objetivo, o projeto conta com a análise de tópicos como: tecnosolucionismo; funcionamento da tecnologia de reconhecimento facial; e análise da aplicação da FRT nas ruas uruguaias e brasileiras.

Desse modo, o projeto se divide em quatro tópicos principais. O primeiro tópico dirá respeito ao uso das tecnologias de segurança como forma de solução para as demandas da Segurança Pública, em especial, a relação entre o combate aos crimes violentos e o discurso tecnosolucionista.

No segundo tópico, será analisado o *modus operandi* da tecnologia de reconhecimento facial, destacando-se principalmente as suas dificuldades operacionais, bem como os vieses raciais e de gênero.

Quanto ao terceiro tópico, este será dedicado à inserção da tecnologia de reconhecimento facial na segurança pública uruguaia. Neste tema, será explorado o processo de aquisição da FRT no Estádio Centenário, bem como o procedimento de licitação decorrente da aquisição de câmeras de reconhecimento facial para o uso nas ruas públicas. Tais aquisições serão contrastadas com a *Ley de Proteccion de Datos Personales (LPD)*, a fim de se verificar possíveis violações aos direitos de privacidade dos usuários. Por fim, será abordado o processo judicial decorrente do processo de aquisição das câmeras.

No último tópico, será avaliado o contexto de aquisição da FRT no cenário brasileiro, em especial o seu uso no Estado do Ceará. Nesse tópico, será comparado o uso dessas tecnologias, com os seus respectivos custos e riscos, com destaque para a ponderação do uso dessas ferramentas em contraponto à LGPD.

A partir do estudo proposto, será possível traçar uma análise multidisciplinar do tema do uso da tecnologia de reconhecimento facial na segurança pública, partindo da compreensão da tecnologia como uma solução para as demandas de segurança para finalmente chegar ao funcionamento da tecnologia, seus riscos para os direitos dos civis e custos. Para chegar a esse feito, o trabalho conta com a metodologia qualitativa dedutiva, bem como a análise bibliográfica correlata aos temas indicados. Destacam-se ainda as limitações provenientes dos tópicos referentes às análises de caso concreto, haja vista que as informações disponibilizadas ao público são escassas e incompletas.

2. SEGURANÇA PÚBLICA E A TECNOLOGIA

Desde o início da implementação das tecnologias de videomonitoramento no Brasil, a tecnologia mostrou-se como uma ferramenta necessária para o avanço e modernização do policiamento nas ruas. O discurso do Comandante Geral da Polícia Militar do Estado do Rio de Janeiro em 2019, Coronel Rogério Figueiredo, traduz bem a imagem que esse investimento na tecnologia projeta: "É a modernidade, enfim, chegando [...] A ferramenta é fantástica. Já passou da época de a PM se modernizar" (Figueiredo, 2019 *in* Edler Duarte, 2024, p. 2).

Entretanto, é necessário adequar as ferramentas tecnológicas aos usos e contextos propostos. E esse não foi o caso da tecnologia adotada pela polícia do Rio de Janeiro. No relatório do Centro de Estudos de Segurança e Cidadania, foi indicado que o *software* utilizado nas câmeras de videomonitoramento nas áreas de Copacabana e arredores do estádio do Maracanã apresentou falhas severas: beira 63% o número de casos em que os indivíduos abordados foram identificados de maneira equivocada, ou seja, as taxas de "falsos positivos" eram alarmantes (Edler Duarte, 2024, p.2). Em outras palavras, o sistema, além de ter demonstrado eficácia em menos da metade dos casos, causou constrangimento aos transeuntes que foram identificados de maneira equivocada.

A princípio, é de se esperar que um *software* com altos índices de erros não possa ser tido como bem-sucedido. Todavia, o uso dessas ferramentas na segurança pública desafia essa lógica. As falhas são ponderadas com os ganhos que se esperam da ferramenta. Nos "discursos tecnocráticos", qualquer estado, por mais endividado que esteja, pode ter acesso a um mecanismo que irá otimizar o trabalho da segurança pública: por meio de tecnologias que buscam "fazer mais com menos", as vantagens do produto são refletidas na melhoria do desempenho e modernização da administração policial (Edler Duarte, 2024).

Com argumentos de otimização dos recursos já existentes e dos procedimentos, os ganhos ludibriam os consumidores. Assim, não se medem esforços para adaptar o corpo policial às exigências da modernidade. Forja-se a necessidade de que aparatos de vigilância precisam passar por um *upgrade*, em que o investimento nas ferramentas de videovigilância se destaca. Com um projeto que busca a eficácia ao aumentar a sua rede de abrangência, ferramentas como o reconhecimento facial passam a ser necessidades fortemente sentidas ao ponto de "entorpecer" as pessoas: torna-se comum e legítimo ser rastreado, bem como ter os dados constantemente analisados, comparados e modificados (Zuboff; Bruno, 2018).

É uma via de mão dupla, as companhias e empresas de tecnologia vendem o produto e os estados os compram. Principalmente no caso da América Latina, que se apresenta como um mercado em expansão para o aprimoramento do *know how* das empresas de tecnologia. Trata-se de uma oportunidade para otimizar os produtos fornecidos, haja vista que é comum as empresas de Big Tech ofertarem ferramentas genéricas e "empurrá-las" para os usuários ao longo do globo: com o acesso aos dados gerados pelos consumidores locais, os hábitos regionais são absorvidos e usados para treinar os algoritmos; consequentemente, com o aperfeiçoamento do desempenho das ferramentas, se espera alavancar na margem de lucro da companhia (Lee, 2019).

Nesse sentido, as tecnologias de vigilância fomentam uma indústria altamente lucrativa e "intimamente" conectada aos governos que a contratam: formam uma teia complexa que intercala condições econômicas e políticas e as traça na cultura de vigilância, por intermédio da dependência e poder político-econômico (Lyon; Bruno, 2018).

O incentivo à aquisição das tecnologias de videomonitoramento na segurança pública tem sido tamanho que chegou-se ao ponto das ferramentas se "camuflarem" na vida cotidiana dos cidadãos. As câmeras tornaram-se invisíveis e passam despercebidas aos olhos humanos, em que o "desaparecimento da tecnologia é o seu ápice de desenvolvimento, já que não seria mais possível distinguir a realidade virtual e o mundo real, qual o aparato que se conecta a quê?" (Scherch, 2024, p. 25). E nessa "onipresença" das câmeras, a *internet* das coisas conecta computação e ambiente, "datifica" as informações, em um movimento guiado pelo imperativo da predição (Scherch, 2024). Essas câmeras invisíveis passam a ser capazes de mapear e prever o comportamento daqueles que são flagrados.

Um exemplo que ilustra esse contexto é a recente aquisição da *Polícia Nacional del Uruguay*. Em 2023, foi anunciado que as ruas da capital Montevidéu passariam a contar com seis mil câmeras espalhadas nas regiões de grande fluxo: destacou-se que o diferencial de tais câmeras de vigilância estaria na IA utilizada nos algoritmos da ferramenta, em que seria possível detectar os movimentos corporais cadastrados como "suspeitos"; tais câmeras também iriam permitir a imediata comunicação ao efetivo policial, quando localizassem tais atividades desviantes (Subrayando, 2023). A confiança no funcionamento da ferramenta é tamanha que, ao revés do que se espera de uma política pública, não há registro publicizado de qualquer relatório de impacto e desempenho que indique a atuação dessas tecnologias voltadas para a modernização da segurança pública (Gonçalves Feliz; Duarte, 2024).

Essa confiança desmedida nas ferramentas tecnológicas pode ser explicada por meio do ofuscamento do debate frente ao seu "brilho". O videomonitoramento se apresenta como uma tecnologia que é familiar, ao ponto de ter sido "domesticada" pelo cotidiano, embora, na sua raiz, tenha sido difundida por meio do medo e desejo de vigilância (Lyon; Bruno, 2018). Ao fim, tornou-se uma realidade pautada pelo fascínio irresistível do controle e predição.

Nesse sentido, torna-se aceitável uma tecnologia com índices de eficácia tão baixos. Essa tecnologia possui um grau de aceitação tão amplo, que passa a ser assimilada pelo modo de vida dos cidadãos: chegou-se ao ponto de a tecnologia na vigilância ser um desejo (Lyon; Bruno, 2018) ou uma exigência.

Todavia, esse desejo pungente pelo aperfeiçoamento dos mecanismos de segurança também mascara uma outra arena de disputa, a do direito de não ser visto. Na negociação com os estados que adquirem a tecnologia de reconhecimento de imagens, há um tópico crucial e pouco discutido: como ficam as delimitações de zonas de privacidade? Aqui, a discussão em torno da vigilância determina a zona fronteiriça entre os que serão vigiados ou não:

> "O trabalho da vigilância, ao que parece, não é corroer os direitos de privacidade, mas sim redistribuí-los. Em vez de um grande número de pessoas possuindo alguns direitos de privacidade, esses direitos foram concentrados no interior do regime de vigilância. Os capitalistas de vigilância possuem amplos direitos de privacidade e, portanto, muitas oportunidades para segredos. Estes são cada vez mais utilizados para privar as populações de escolha no que diz respeito a que partes de sua vida desejam manter em sigilo (...)" (Zuboff; Bruno, 2018, p. 48).

Nesse ponto, as discussões para a aquisição da tecnologia passam a ser quase unilaterais. Os "capitalistas da vigilância" se aproveitam do abismo informacional ao lançarem mão de seus produtos aos países consumidores com baixa compreensão pública sobre o funcionamento das tecnologias de reconhecimento de imagem e regulamentação deficitária do tema: a margem de lucro reside na exploração desse "lapso social" (Zuboff; Bruno, 2018). Tais contratações são ágeis e logo se observa o produto delas nas ruas.

Desse modo, a paisagem muda e os espaços públicos passam a ser povoados por essas câmeras invisibilizadas. Todavia, as informações capturadas por essas máquinas se traduzem em um emaranhado confuso de conexões. Os sistemas de videomonitoramento atuam de maneira esparsa, desconexa e "pulverizada", ao ponto de não ser possível identificar quais são os sistemas, quem os controla, os responsáveis por seu monitoramento e como eles operam (Firmino; Bruno, 2018). É um contexto complexo em que são levantados questionamentos quanto aos limites e extensão territorial das câmeras de reconhecimento de imagens nas ruas.

Para compreender onde a zona limítrofe da permissão de atuação dos sistemas de videomonitoramento se encaixa, é necessário investigar as raízes da adesão cega ao imperativo da modernização da vigilância pública.

2.1. Tecnologia e o tecnosolucionismo

Inicialmente, a "modernização" das forças policiais identificou-se como um recurso argumentativo, para enfim ganhar destaque nos debates e discursos públicos. O tema apresentou-se como um "refinamento" das questões levantadas pela discussão das soluções e causas da criminalidade urbana e persistência da violência, sendo utilizado como um contraponto no embate entre os garantidores da "lei e da ordem" e os "defensores dos direitos humanos" (Ribeiro, 2024). Com suas raízes nas "demandas acumuladas e incompletas", o investimento nas tecnologias de segurança é caracterizado por soluções de natureza reativa e esparsas que se apresentam "imediatas": seja por meio de "melhores resultados", índices ou eficiência do trabalho policial (Ribeiro, 2024).

Ocorre que, conforme destacado no capítulo anterior, esses *upgrades* se direcionaram para um grande objetivo: vigiar e prever. O desenvolvimento dos aparatos tecnológicos de videovigilância permitiu uma atualização nas formas de policiamento, que então passaram a usar a lógica atuarial para sistematizar as informações relativas aos grupos de risco e gerenciá-los: com a criação de "rótulos populistas" para classificar os indivíduos e usar os dados para elaborar diagnósticos e estatísticas (Dieter, 2012 *in* Ribeiro, 2024).

O objetivo desse redesenho da lógica criminal pode ser ilustrado no zoneamento da vigilância, bem como na definição do grau de securitização de cada área. São definidas regiões de monitoramento onde os comportamentos dos transeuntes são mapeados e vislumbrados de forma cristalina:

> "Aos olhos da vigilância, da segurança e dos sistemas de controle, tudo se torna transparente, enquanto na rotina diária material, mundana e ordinária, fronteiras tornam-se incertas e intangíveis, mas ao mesmo tempo mais agressivas e seletivas. Existe uma sobreposição de limites físicos e digitais que define níveis de controle nos territórios sociopolíticos da cidade. Assim, parece justo afirmar que espaços cada vez mais controláveis estão determinando como a terra é ocupada ou reocupada nas cidades" (Firmino; Bruno, 2018, p.87).

Na lógica da predição estatística, alguns questionamentos devem ser suscitados. Inicialmente, a definição dessas zonas de risco e, por fim, a consequência desses rótulos e o uso que se dá para as informações coletadas.

Todavia, o que se percebe dessa nova roupagem do poder punitivo é que a validade das informações que venham a compor registros como o Inquérito Policial passa pela "gestão da informação" (Duarte, 2017):

> "(...) As polícias se comunicam por aplicativos, invadem celulares de cidadãos (ou não cidadãos), fazem uso extenso da internet e de sistemas informacionais, porém, tudo termina, ali, na forma escrita capaz de impedir o registro de todas as ações anteriores. Poucas, raras e clandestinas, são as imagens das ações policiais. Nenhuma transparência do fluxo de decisões: quando se decidiu investigar alguém, o que motivou a abordagem, quem são os personagens, qual a cadeia de comando?" (DUARTE, 2017, p. 25-26).

Em outras palavras, a prática cotidiana pulveriza as respostas inconvenientes ao funcionamento e uso das tecnologias de monitoramento. Os dados não registrados acabam excluídos do relatório e logo são esquecidos no emaranhado confuso da teia de informações. Contudo, tal situação de escassez inerente à operacionalização das tecnologias de segurança contrasta com a forte propaganda lançada para divulgar o uso das mesmas tecnologias.

Como um movimento político, a atualização das forças de segurança faz bom uso da oportunidade proporcionada pelo contexto social de insegurança pública e violência criminal na propaganda tecnosolucionista: tal divulgação conta com a massiva exposição midiática, como "forma oficial" de se vincular as informações relativas ao funcionamento e uso da tecnologia adotada (Ribeiro, 2024). Ocorre que, para além da propaganda, não há sequer informações básicas quanto ao funcionamento da tecnologia.

Trata-se, pois, de uma "estratégia simbólica" que faz uso da "parcial transparência" e "filtragem" das informações, com a finalidade de garantir a "custódia informacional" (Ribeiro, 2024) dos processos e resultados. Nesse sentido, a divulgação da modernização das tecnologias de segurança não pode ser vista apenas como uma estratégia de *marketing.*

Para além da publicização do uso de novos aparatos tecnológicos e sua consequente politização, destaca-se que o seu uso não se restringe à forma instrumental das máquinas. Pelo contrário, esse movimento faz parte de um processo sustentado e promovido por uma complexa teia de necessidades locais atreladas aos discursos dos "emissários políticos" e à pauta neoliberal: como uma estratégia de punição dos grupos "perigosos" (Ribeiro, 2024).

Nesse cenário, essa cadeia de necessidades estruturantes do meio social, estruturada pelas demandas fabricadas pela agenda das Big Tech, sustenta-se no deslumbramento com a tecnologia e sua autolegitimação. Aqui, o embate entre os "garantidores da lei e da ordem" e os "defensores dos direitos humanos" é decidido no efeito ofuscante da tecnologia.

Tal constatação pode gerar espanto, todavia um efeito próprio das tecnologias de vigilância é que se imagina que elas não precisam ser legitimadas. A aparência da modernização da segurança pública é ensurdecedora e aplaudida: o progresso que as novas tecnologias representam tornou-se fundamento para sustentar a sua "assimilação" pela administração pública; a eficiência, celeridade e neutralidade prometidas mostram-se como suficientes para legitimar o uso da ferramenta tecnológica (GARCIA, 2017).

Entretanto, os argumentos que sustentam esse *marketing* do uso das tecnologias de segurança enfrentam o desafio da falha. Os dados capturados e registrados, conforme a lógica atuarial de gerenciamento de grupos de risco, por vezes apresentam desconexões e resultam em elevadas margens de erro. Tendo em vista esse contraponto à eficiência das máquinas, cabem ainda algumas breves considerações sobre a análise da "falha" da videosegurança.

2.1.1. A falácia da falha

Ante a eficiência presumida das decisões tecnológicas, como explicar o exemplo citado na introdução, em que o *software* contratado pela Polícia do Rio de Janeiro apresentou péssimo desempenho em 63% dos casos? A resposta está no jogo argumentativo da falha.

A tecnologia não pode apresentar respostas equivocadas, de modo que é comum concluir que o problema para o seu funcionamento está na forma como o sistema foi operacionalizado: seja na infraestrutura, falta de recursos ou no gerenciamento das ferramentas. Em outras palavras, a tecnologia seria moderna demais para o uso. Ocorre que esse tipo de argumento "crítico" focado na essencialização do atraso do país e que atribui os erros aos desvios de funções, alta burocratização e a incapacidade de articulação das políticas regionais desvirtua o debate (Edler Duarte, 2024). Negligencia-se assim o fato de que os países "periféricos", como os da América Latina, são usados como arenas de testes dos dispositivos de controle social: em que o uso desses países como "laboratórios" permite o controle e modelagem dos aparatos e saberes de repressão das populações subalternizadas, a fim de melhor rotulá-las e segregá-las (Edler Duarte, 2024).

Nesse sentido, a "falha" dos países do sul global é explorada e monetizada. Opera-se, então, com a "noção produtiva" da falha, pois é com a identificação e ponderação das falhas que se aprimoram as tecnologias e se otimizam os produtos vendidos (Edler Duarte, 2024). Basta adaptar o algoritmo que se resolve a falha.

Destaca-se ainda que, mesmo que a empresa produtora da tecnologia não conte com a engenharia de ponta e o "conhecimento de elite" (Lee, 2019) para desenvolver a IA dotada de perfeição, uma alternativa para esse déficit seria a implementação e experimentação do produto: "(...) essa implementação terá o efeito colateral de levar a um crescimento mais exponencial no acúmulo de dados e um avanço correspondente no poder da IA por trás dela" (Lee,2019, p. 150).

O uso dos algoritmos em tempo real nas câmaras de vídeo segurança proporciona uma "base estatística" dos dados coletados a cada segundo, ao ponto de que eventual "falha" ou "falso positivo" é reflexo da "plasticidade" da tecnologia: haja vista que a mesma segue a "(...) lógica de rastreamento mais do que de diagnóstico, o objetivo é não deixar escapar nenhum positivo verdadeiro, qualquer que seja a taxa de falsos positivos" (Rouvroy; Berns; Bruno, 2018, p.117). A falha é parte constituinte do funcionamento da tecnologia.

Em outros termos, explorar a falha proporciona uma oportunidade de alavancar os lucros com a venda e uso dos produtos decorrentes das tecnologias de vigilância. Contudo, essa não é a razão de ser da falha. A falha, como lucro, também reflete na manutenção da falha. É um movimento cíclico.

Nesse contexto, ao focar o debate da falha como mero empecilho para a eficiência, a potencialidade da sua manutenção enquanto fonte de lucro é ignorada. Igualmente negligenciada é a exploração da ideia da falha para "(...) reduzir direitos, ignorando que os meios de opressão e exclusão que se perpetuam através das falhas são inerentes a seu contexto operacional e à forma como a indústria estabelece prioridades (...)" (Edler Duarte, 2024, p.10). Desse modo, manter a falha faz parte de uma "ignorância estratégica" com vistas a legitimar práticas discriminatórias nas relações de poder e produzir a violência contra grupos marginalizados (Edler Duarte, 2024). E essa "ignorância estratégica" é operada principalmente pela falta de planejamento e organização da gestão das tecnologias de vigilância. Haja vista que é imprescindível ao bom funcionamento e adaptação das inovações tecnológicas às necessidades e realidades locais o uso de abordagens colaborativas entre governo, empresas, sociedade e academia (Ferreira; Novaes; Macedo; 2023).

Em síntese, a falha faz parte de uma estratégia pautada em sistemas desconexos, redes de informações sem vigilância, dados perdidos e ausência de transparência. A falha, enquanto um elemento da "margem de erro" da lógica atuarial, é produzida e determinada pelo contexto socioespacial em que a tecnologia. Ao ponto que reforça a necessidade de investimento nas políticas de controle.

E é na produção dos discursos de que algumas regiões precisam ser vigiado e certos grupos controlados, que se reforça a atuação "(...) ostensiva da polícia nas comunidades com base no perfil de risco imputado aos moradores do lugar" (Santos Costa, 2021, p. 76). Trata-se de um movimento cíclico de produção de falhas e demandas.

No bojo da discussão da intersecção da segurança pública e atuação dos discursos tecnosolucionistas na criação de demandas e necessidades, o último tópico deste capítulo será dedicado ao estudo de dois casos: o Centro de Operações Rio e o Estádio Centenário.

2.1.2. Centro de Operações Rio e Estádio Centenário

Com vistas a atender os anseios elencados no "Padrão FIFA", os megaeventos realizados no Rio de Janeiro, como os Jogos Pan-Americanos, a Copa do Mundo e as Olimpíadas, a cidade do Rio de Janeiro (BR) precisou "modernizar-se" a fim de proporcionar maior segurança durante as competições (Cardoso, 2013). Ao sediar esses megaeventos, a cidade tornou-se laboratório na tentativa de tornar-se uma cidade inteligente (*smart city*).

Financiada com um grande "fluxo" internacional de transferências de recursos, a segurança pública do Rio passou a contar com aparatos tecnológicos de ponta e altamente especializados (Cardoso, 2013). E, para gerir as novas ferramentas de vigilância, criou-se o Centro de Operações Rio (COR) que: "(...) reúne a ambição tanto de ver a partir de distintas perspectivas (sobrevisão) quanto de ver adiante no tempo (antevisão)" (Bruno, 2018, p. 240-241). Com o sistema operado no COR, a cidade passou a ser vista por meio de uma parede de vidro, na qual abas de informação convergem para mapear e diagnosticar a correlação entre as informações obtidas pelas 900 câmeras espalhadas em torno das regiões de maior movimento na cidade em conjunto com os dados coletados em aplicativos como Waze e Twitter (Bruno, 2018). Por meio do *software* utilizado nas ferramentas de vigilância, a tela do COR ilustra o monitoramento "inteligente" das ruas.

A sensação de segurança proporcionada pelas ferramentas indica um fomento à esperança, esperança de que os custos sejam refletidos em gastos necessários, bem como que "os problemas sociais" sejam solucionados: ainda, que tais aparatos tenham sido adquiridos em licitações superfaturadas, repletas de ilegalidades e indícios de corrupção (Cardoso, 2013).

Em outros termos, o que justifica a crença de que os gastos volumosos nos megaeventos tenham valido a pena traduz-se no discurso do "legado" deixado pelas competições: que se reflete no anseio pela modernização da cidade e do país, rumo ao horizonte projetado pelo paradigma europeu; assim como na infraestrutura de vigilância proporcionada "deixadas" pelos eventos (Cardoso, 2013).

Com o investimento na modernização do sistema de segurança pública, o Rio estaria mais perto do horizonte projetado pela sombra dos países do Norte.

Como uma cidade mais inteligente, *smarter*, o Rio de Janeiro passou a ser incluído nas narrativas da gestão inteligente da vida urbana e eficiência dos processos (Firmino; Bruno, 2018) por meio da incorporação dos aparatos "modernos" no monitoramento. Todavia, essa gestão eficaz e integral da rotina urbana depende da articulação de redes e atores.

Tal articulação faz-se possível por meio da criação de "zonas tecnológicas" em que os dados gerados pela mediação algorítmica da informação são coordenados e distribuídos pelas conexões: esses dados circulam em espaços destituídos de espaço físico ou território próprio, mas sim, redes que capturam os fluxos de informações (Cardoso, 2013). Entretanto, as informações que veiculam nesse emaranhado de redes podem ficar ininteligíveis para alguns operadores. A falta de comunicação e de uma "linguagem comum" entre os diferentes sistemas de segurança dificulta a atuação das partes interessadas, haja vista que nessa teia tecnológica há estratégias de monitoramento regionais e softwares com padrões próprios (Cardoso, 2013). Sem a coordenação dos elementos da zona tecnológica, a gestão eficiente prometida pela modernização encontra um sério empecilho.

Além da falta de coesão entre as ferramentas do sistema de segurança, outro ponto que deve ser suscitado na análise da *smarter city* é a definição de fronteiras:

> "(...)O funcionamento dos sistemas informáticos precisa, então, ser aberto o suficiente para que a comunicação interinstitucional integre os diferentes atores responsáveis pela segurança pública no Rio de Janeiro, mas ao mesmo tempo deve ter um grau considerável de fechamento para que seja protegida a confidencialidade daquelas informações e minimizada a vulnerabilidade do sistema diante de suas principais ameaças externas, assim como para manter uma mínima autonomia das instituições". (CARDOSO, 2013, p. 139).

Nesse sentido, definir os pontos de entrada de informação e quem tem acesso faz parte do processo de formação de barreiras do sistema. Tornar o sistema invulnerável ao restringir os pontos fragilizados é visto como uma condição necessária para evitar vazamentos de dados. Entretanto, tais barreiras externas devem ser olhadas com desconfiança.

Nas “estruturas tecno-informacionais” os dados coletados pelas tecnologias, em especial as de videomonitoramento, estão sob o monopólio dos atores e agentes que detém o “capital informacional”: de modo que requisições de acesso às informações básicas relativas aos procedimentos, formas de uso das ferramentas na rotina policial e os dados gerados por esses processos, tudo isso leva a informações “opacas”, parciais e desconexas (Ribeiro, 2024).

As ditas barreiras de segurança acabam por transformar as “zonas tecnológicas” em verdadeiras caixas-pretas. Essa desconfiança na forma como as ferramentas de vigilância operam pode ser melhor traduzida no exemplo prático de uma busca no sistema do COR.

Com sua tela plana repleta de informações sobre os pormenores da cidade, o Centro de Operações Rio possui uma visão panorâmica da vida cotidiana da cidade. Nessa tela aparecem informações provenientes da “mineração” dos dados de radares de trânsito, informações meteorológicas, base de dados sobre populações em áreas específicas, defesa civil, serviço de eletricidade, gás e redes sociais como Waze e Twitter, tudo isso apresentado em uma linha do tempo que indica diagnósticos de “normalidade”, “atenção” e “crise” (Bruno, 2018). Chama a atenção o fato de que mensagens publicadas em redes sociais são utilizadas como fonte de dados para a elaboração de relatórios:

> “(...) Numa visita recente ao COR, um técnico responsável pela apresentação do painel georreferenciado mostrou como é possível selecionar uma determinada área da cidade nesse painel, visualizar e “minerar” nela uma série de dados, entre os quais o que as pessoas estão, por exemplo, postando no Twitter naquela área. O técnico seleciona um tema qualquer, de sua escolha – no caso, ‘acidente’ –,e na barra esquerda da tela, ao lado da imagem-satélite da região selecionada, visualizamos todas as postagens que tinham partido de dispositivos com geolocalização ativa no local, contendo a palavra ‘acidente’” (BRUNO, 2018, p. 244).

O exemplo do funcionamento do COR lança luz ao fato de que as informações publicadas pelos usuários das mídias sociais são alcançadas pelo sistema de segurança pública, ao ponto de serem usadas como fonte de dados. Todavia, esse movimento ocorre sem que o cidadão tenha sequer ciência do uso atribuído aos seus dados. Trata-se de um exemplo que escancara a “assimetria de visibilidade e de escala”: na primeira, inexiste qualquer transparência quanto ao uso e funcionamento da tecnologia, as informações são “opacas”; na segunda, falta a compreensão da escala, limites, da abrangência do controle e vigilância, ao ponto de ser extremamente difícil precisar onde ela começa ou termina (Bruno, 2018).

No bojo da discussão entre os limites da tecnologia e o seu uso, ainda cabem alguns breves comentários sobre o uso tecnosolucionista de uma ferramenta ineficaz. Diferente do exemplo do s*oftware* utilizado pela Polícia do Rio de Janeiro para monitorar os arredores do estádio Maracanã e na região de Copacabana, o exemplo abaixo não trata de "falsos positivos", mas sim do fato de não haver sequer registros técnicos de que a ferramenta cumpriu com seu objetivo básico.

A implementação da tecnologia de reconhecimento facial nas câmaras de vigilância do Estádio Centenário, localizado na capital uruguaia, foi marcada por articulações políticas em meio ao cenário de terror proporcionado pela violência das torcidas nos estádios. Em 2016, os jogos da final da Liga Uruguaia tiveram de ser interrompidos devido à invasão de torcedores no estádio e o depredaram, houve registro de arremesso de botijão de gás nos funcionários; todavia, episódios como esse são frequentes nos noticiários uruguaios, somando-se ainda à pauta os registros semanais de agressões aos árbitros e arremesso de projéteis no campo (Gonçalves Feliz; Duarte, 2024). Nesse ínterim, a segurança nos estádios passou a ser uma pauta disputada na arena política.

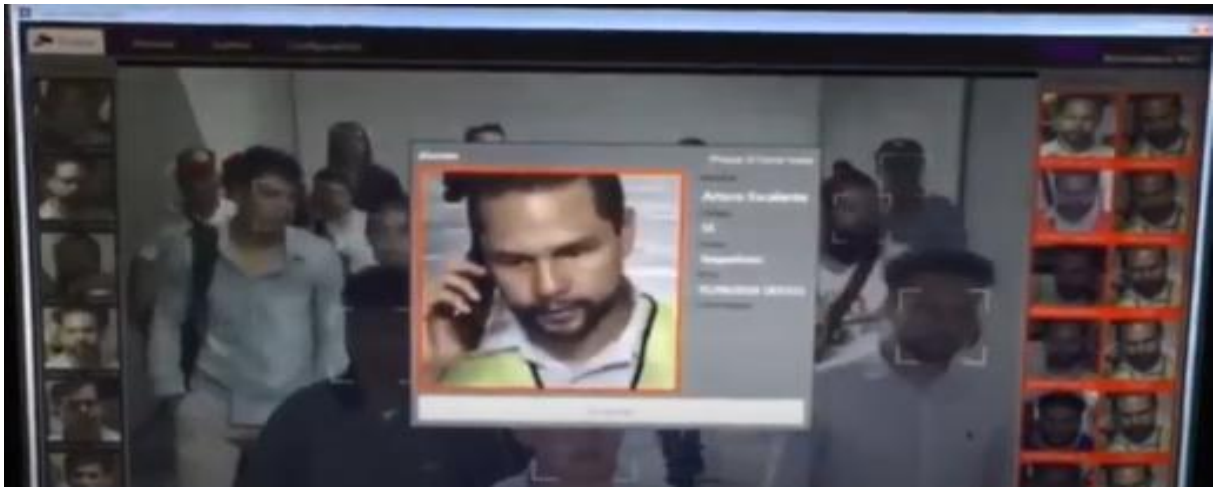
Apesar da movimentação da AUF (Asociación Uruguaya de Fútbol) para realizar a contratação de ferramentas de videomonitoramento, não tardou para que o *Ministro del Interior*, Eduardo Bonomi, assumisse o protagonismo na mediação e contratação da tecnologia de reconhecimento facial: ao associar a perpetração da violência nos campos às torcidas, *hinchas*, violentas (*barras bravas*), determinou os requisitos de funcionamento dos *softwares* a fim de melhor identificar os membros das hinchas violentas (Gonçalves Feliz; Duarte, 2024). Entretanto, as informações que dizem respeito ao funcionamento e desempenho dessa tecnologia são escassas, ao ponto de poderem ser reduzidas a dois grupos de notícias: licitação sobre o processo de contratação da empresa fornecedora de energia; anúncios genéricos do *software* utilizado.

No que diz respeito ao primeiro grupo, só se sabe que a empresa fornecedora DDBA, vinculada à HERTA, foi selecionada por apresentar índice de acerto de 99,8% nos horários diurno e noturno (Gub.Uy, 2018). Se a empresa de fato atendeu esse requisito, não tem como ser atestado, tendo em vista que não há registro publicizado da análise de desempenho da ferramenta de reconhecimento facial utilizada. Quanto ao último grupo de informações, inicialmente destaca-se a fala do responsável por intermediar a contratação da DDBA, o subsecretário do *Ministro del Interior*, Jorge Vásquez: *"Hace dos años que no se registran episodios de violencia en los espectáculos deportivos, tanto en el fútbol como en el básquetbol"* (Vásquez 2018 *in* Gub. Uy, 2018).

Na oportunidade, também destacou que só houve registro de uma “detecção errônea” no decurso desse mesmo período (Gub. Uy, 2018). Igualmente, não foram demonstrados relatórios de desempenho ou explicações quanto aos casos de “falso positivo” e “falso negativo”, que é quando a ferramenta deveria identificar o indivíduo e selecioná-lo, mas não o faz.

Ainda no último grupo, destaca-se a propaganda realizada pela AUF sobre o software utilizado no Estádio Centenário. Em sua conta no YouTube, a AUF TV (2017), foi feita a postagem de um vídeo demonstrativo do sistema de câmeras de reconhecimento facial:

Figura 1 - Imagem da tela do operador da ferramenta de reconhecimento facial. Min: 0:10



Fonte: AUF. TV

O vídeo possui 25 segundos de duração e demonstra o processo de identificação de alguns rostos dos transeuntes que entraram no Estádio Centenário. Não conta com áudio ou legendas explicativas. Na imagem, é possível ver um indivíduo sendo selecionado e um quadro com informações ininteligíveis. Na lateral esquerda, é possível vislumbrar os indivíduos que já tiveram a face registrada e na lateral direita um quadro que se divide em dois: na esquerda, os rostos dos transeuntes que ficaram registrados e na direita, a imagem de um indivíduo que se busca selecionar; essa imagem de um indivíduo “buscado” é submetida às variações de luminosidade e nitidez.

Destaca-se que os apontamentos feitos se deram pela observação do vídeo da AUF TV. Também é importante salientar que na legenda do vídeo, bem como em qualquer outra mídia de comunicação da AUF, não há registro da forma como a FRT opera.

Ou seja, as informações básicas devem ser deduzidas. Nos anos subsequentes, não há divulgação do desempenho da ferramenta. Todavia, a prometida redução dos índices de violência e identificação dos membros das *barras bravas* mostrou-se sem respaldo concreto. As agressões aos árbitros e jogadores ainda persistem, ao ponto de que, em 2022, os jogadores das ligas profissionais paralisaram os jogos e, em 2023, a categoria dos árbitros emitiu uma nota pública indicando greve, frente ao "perigoso costume"[1] das agressões e falta de punição rigorosa (Gonçalves Feliz; Duarte, 2024).

Em suma, os dois exemplos elencados se destacam por ilustrar o quão destoante é da realidade a promessa de que as novas ferramentas tecnológicas operariam rumo à salvação da segurança pública. No primeiro caso, o *software* utilizado não possui limites, barreiras como a privacidade dos cidadãos são ultrapassadas em segundos, sem que os mesmos tenham sequer a possibilidade de questionar o uso da ferramenta, pois desconhecem a sua existência. Já no último exemplo, o *surf* na onda da comoção popular resultou em discursos sem respaldo técnico. Entretanto, apesar de tratarem de realidades diferentes, ambas as tecnologias de reconhecimento facial possuem um ponto em comum: a falta de transparência. Nesse sentido, a próxima seção irá se dedicar a compreender o funcionamento dessa ferramenta, bem como apontar os seus vieses.

[1] No estudo de Gonçalves Feliz e Duarte (2024), os autores indicam um quadro comparativo das infrações cometidas em campo, nos principais estádios uruguaios, no período de 3 meses no ano de 2023 e 2024. Os dados indicam que infrações referentes às agressões apresentam elevadas ocorrências em tão curto período de tempo, ainda que impactam em punições severas aos cofres dos times como desconto nos valores recebidos nas transmissões de TV e jogos sem público pagante. Os autores concluíram que a punição não se mostrou suficiente para impedir os *barras bravas*, pelo contrário, incentiva a participação destes em campo.

3. O RECONHECIMENTO FACIAL

Conforme demonstrado anteriormente, as tecnologias de reconhecimento de imagens representaram foram calorosamente recebidas pelos discursos tecnosolucionistas. Dentre eles, destaca-se a articulação do reconhecimento facial como forma de proporcionar mais justiça. E o que sustentaria esse anseio popular é a promessa de que a FRT atuaria como um instrumento apto a garantir a execução penal, pois, ao localizar os infratores, iria evitar a prescrição intercorrente ou a própria prescrição da pretensão executória (Andrea; Silva; Gundim; 2022). Tal argumento se sustenta na premissa de que, ao monitorar as ruas e registrar os rostos de todos os transeuntes que por lá eventualmente passarem, em algum momento o infrator, o "suspeito", será identificado pelo algoritmo e selecionado.

A FRT também está relacionada à máxima eficiência de recursos. Com a adesão das câmeras de vigilância, os governos estaduais e municipais veem nas câmeras a substituição de grandes efetivos policiais nas ruas (Ferreira; Novaes; Macedo; 2023). Ademais, além de proporcionar a sensação de segurança aos cidadãos, essa tecnologia auxilia na tomada de decisões e "gestão das cidades", pois os dados do "processo de vigilância" podem ser convertidos em relatórios disponíveis para consultas e análise de lacunas (Ferreira; Novaes; Macedo, 2023). Em outros termos, a câmera acompanha a cidade, protegendo-a, ao passo que registra as suas conclusões em relatórios.

Desse modo, as tecnologias de reconhecimento de imagens são ferramentas usadas no processo decisório e que formulam decisões em questão de segundos: tais como selecionar ou não o indivíduo. Nesse sentido, é necessário compreender a forma como a máquina fria chega a essas conclusões e até que ponto essa análise parte de premissas inseridas pelos programadores ou observadas no ambiente prático.

Delineando o funcionamento da FRT, oportuna faz-se a comparação entre máquinas e organismos vivos realizada por Norbert Wiener (1968). Para o autor, a exemplo do comportamento dos seres vivos, alguns tipos de máquinas poderiam ser ensinados a modificar os seus padrões de resposta e comportamento com base nas experiências passadas, a fim de direcionar-se com mais eficiência em eventos futuros (WIENER, 1968). Aqui as informações inseridas são orientadas pelo "fluxo" já programado, mas também acabam por impactar no seu desempenho e resultado programado, eis, assim, o fenômeno da alteração de desempenho pela realimentação do sistema:

> “Repito: a realimentação é um método de controle de um sistema pela reintrodução, nele, dos resultados de seu desempenho pretérito. Se esses resultados forem usados apenas como dados numéricos para a crítica e regulagem do sistema, teremos a realimentação simples dos técnicos de controle. Se, todavia, a informação que remonta do desempenho for capaz de mudar o método e o padrão geral de desempenho, então teremos um processo a que poderemos denominar aprendizagem” (WIENER, 1968, p. 50).

A razão dessa modificação no padrão de respostas pode ser explicada com a comparação dos sistemas da máquina ao sistema nervoso. Por meio de conexões que transmitem a informação para o resultado "movimento", o impulso direcionado pelas sinapses deve ser forte o suficiente para ser transmitido. Aqui se opera a lógica do "tudo ou nada", ou seja, o problema da transmissão dos impulsos depende da combinação das fibras adjacentes, para daí se pensar em um padrão de resposta, tudo isso dentro de um tempo limitado, para evitar que a informação fique estagnada (WIENER, 1968).

Norbert Wiener (1968) ainda destaca as características das máquinas digitais, cuja programação para decidir entre "sim" e "não" proporciona a diferenciação de uma infinidade de dados de maneira rápida e eficiente.

Ocorre que a quantidade de dados inseridos pode alterar o fluxo de informações e, consequentemente, impactar no resultado esperado. Trata-se do fenômeno descrito como *"machine learning"*. Aqui, a máquina se adapta a novos padrões, com base nas informações que são usadas para retroalimentar o seu banco de dados. Quanto a esse processo de aprendizado, o próximo capítulo irá tecer alguns comentários.

3.1. Funcionamento da tecnologia

A máquina não aprende sem estudar o seu material e fazer exercícios. Com sua “mente de criança”, a máquina deve ser submetida a um processo de educação e, para isso, deve contar com a “matéria-prima básica” do aprendizado, os dados (Brandão, 2023).

Os dados são exemplos, amostras, na forma de informação, que são oferecidos ao sistema, a fim de que, nutrido por milhares de exemplos, o sistema possa ser instruído: em outros termos, os dados são a matéria-prima, a fonte de conhecimento da máquina (Brandão, 2023). Para que o processo de aprendizado flua regularmente, a ferramenta deve ser alimentada com as informações, treinada por elas e depois testada.

Nesse sentido, são necessários dois blocos de dados para proporcionar o aprendizado de máquina: os dados de treinamento e os dados de teste.

Os dados de treinamento representam em média 75-80% das amostras e são utilizados para construir um modelo matemático capaz de generalizar a equação dessas informações e treinar esse modelo: já os dados de testes consistem na parcela de informações nunca vistas pelo sistema, cuja função é avaliar o funcionamento da ferramenta (Brandão, 2023).

Nesse processo de "educação", o sistema deve compreender o que é "certo" e "errado" ou chegar a suas próprias conclusões. O último modelo de aprendizado de máquina é comum em sistemas que buscam por padrões e detectam anomalias, são comuns em instituições financeiras, já o primeiro modelo consiste no aprendizado supervisionado (Brandão, 2023). Aqui, o sistema precisa de orientações para identificar a informação relevante:

> "No aprendizado supervisionado, a fase de treinamento deve incluir não somente o conjunto de treinamento, mas também a informação relevante sobre cada exemplo. Normalmente, chamamos essa informação relevante de etiqueta, rótulo ou label. Em outras palavras, para o treinamento fornecemos à máquina o que seria a solução da previsão de cada exemplo. Por exemplo, suponha que a máquina deva reconhecer qual é o algarismo escrito à mão, para isso, devemos antes treiná-la. Neste sentido, é necessário que no treinamento seja fornecido também qual é o dígito em cada imagem" (Brandão, 2023, p. 23).

Por meio dos dados rotulados, o sistema é capaz de compreender as informações relevantes ao ponto de identificá-las nos demais exemplos do conjunto de treinamento. Desse modo, os dados de treinamento integram a base de formação do sistema. Aqui, o conjunto é utilizado para construir o algoritmo fundamental, um modelo estatístico e matemático pré-estabelecido pelo programador que busca generalizar os dados, enquanto aprende com eles novos padrões (Brandão, 2023).

Em outros termos, o sistema de reconhecimento facial é formado por dados que vão constituir a equação fundamental. Aproveitando o conceito de *habitus* em Bourdieu (2007), algoritmo é a estrutura do sistema, enquanto é estruturado pelos dados e possui a característica estruturante em relação às informações que seleciona ou descarta. Todavia, o algoritmo não é somente (re)definido pelos dados, o próprio sistema o estrutura e é por ele modificado.

Uma das subáreas do aprendizado de máquina é o desenvolvimento da aprendizagem profunda, *deep learning*, que é responsável por desenvolver os algoritmos semelhantes às redes neurais do cérebro humano (Vaz Borges Carneiro; Costato, 2023).

Tais algoritmos operam nas redes neurais artificiais, cuja constituição é formada por camada de entrada, saída e camadas escondidas; em cada uma delas haverá uma série de nós; neles ocorre a soma ponderada das relações matemáticas extraídas dos dados, onde, a depender da função estatística do nó, o resultado das somas irá ativá-lo ou não, de modo que, por meio desse processo de ativação de cada um dos nós, a informação é passada da camada de entrada até a camada de saída (Vaz Borges Carneiro; Costato, 2023).

Entretanto, as funções que determinam a "chave" de cada nó não consistem em resultados exatos. Pois os modelos matemáticos utilizados pelos algoritmos do reconhecimento facial operam por meio de funções estatísticas, em que cada dado é um conjunto de probabilidades cujo resultado final representa o equilíbrio dessas somas (ADC, 2019).

Ademais, dentro das camadas múltiplas, "escondidas", o sistema é capaz de selecionar as informações que considera relevantes, antes mesmo de passarem pela seleção dos nós. Por meio do procedimento realizado pelos algoritmos, eles são capazes de identificar padrões hierárquicos nas redes neurais e extrair diretamente dos dados de entrada as informações relevantes ao processo de treinamento, a fim de melhor utilizá-las nas tarefas que foram programadas (Vaz Borges Carneiro; Costato, 2023). Ou seja, a contrario sensu, as informações que não forem pertinentes ao sistema são prontamente descartadas.

Ocorre que o processo de (re)definição do padrão estatístico dos nós requer um volumoso conjunto de dados, o que encarece o processo de desenvolvimento das redes neurais. Entretanto, uma alternativa para reduzir os custos da fase de treinamento da rede consiste em utilizar redes neurais já treinadas previamente, como "ponto de partida" para estabelecer os padrões das funções (Vaz Borges Carneiro; Costato, 2023). Assim, ao adquirir um sistema já configurado com as funções de cada nó, mostra-se vantajoso, ainda mais quando tais redes pré-treinadas já estão disponíveis para utilização pública.

Ante o exposto, alguns tópicos se destacam, principalmente no que tange ao funcionamento do conjunto de dados de treinamento. Pois, ao definir quais dados farão parte dos 80% do banco do sistema, intrinsecamente se define a função fundamental, algoritmo, que irá operar frente aos exemplos apresentados. Ou seja, a montagem desse banco é determinante no funcionamento do sistema de reconhecimento facial, mas não somente isso. O algoritmo fundamental também altera o sistema, na medida em que precisa se adaptar aos novos resultados. É necessário aprender quais somas são úteis e relevantes para ativar o nó, sob pena de confundir a rede neural. E, para manter o equilíbrio do sistema, o algoritmo está disposto a descartar os dados que não apresentem resultados congruentes com o esperado.

Nesse processo de seleção de dados, alguns questionamentos devem ser levantados, o primeiro deles diz respeito à procedência da rede neural, se ela é própria ou adquirida. Outra ponderação a se fazer relaciona-se com a dúvida de quais são as informações descartáveis, aquelas que sequer entram no sistema, bem como se todas as informações "admitidas" pelo sistema possuem a mesma relevância. A presença de camadas escondidas aptas a descartar dados levanta o questionamento quanto à existência de camadas que fazem o oposto, ou seja, que selecionam positivamente uma informação e criam "atalhos" na rede de nós.

As dúvidas são numerosas, ao passo que as respostas nem tanto. Então, para melhor atender a esses anseios, optou-se por sumarizar todas essas ponderações em um único questionamento: o processo de definição de prioridades da rede neural foi escrito ou observado? E, na tentativa de melhor responder a essa pergunta, os próximos capítulos irão se dedicar ao comportamento do sistema de reconhecimento facial ante os cenários de "falhas".

3.1.1. Adversidades relacionadas com a condição de captura do dado

No processo de conversão da imagem em informações legíveis para o sistema, é necessário que sejam atendidas algumas etapas. A primeira delas é a detecção do rosto no ambiente, em que é identificada a face e dela extraída as características principais na forma de vetores, os quais serão capazes de representar a imagem capturada (Vaz Borges Carneiro; Costato, 2023). As demais fases constituem-se em alinhamento, em que a imagem é rotacionada até os olhos ficarem em um ângulo de 180º; representação, em que os vetores são condensados em informações relevantes para o processo de reconhecimento da face; e, por fim, a classificação, a etapa final de determinar a identidade do rosto (Vaz Borges Carneiro; Costato, 2023) e lhe atribuir o rótulo.

Todavia, esse procedimento, em que a imagem passa da camada de entrada até a de saída, onde será rotulada, pode ter complicações, caso a imagem não apresente qualidade. Trata-se da situação em que as imagens capturadas não são nítidas: "borrões" obtidos em tempo real e em distância considerável. Virar a imagem e buscar os vetores principais que a tornam única passam a ser tarefas complexas e propícias a menores taxas de acerto.

Desse modo, é importante que os sistemas das redes neurais estejam preparados para lidar com dados de baixa qualidade, caso queiram ser lançados no mercado. E, para isso, existem testes de ruído que buscam treinar o algoritmo a reconhecer as somas provenientes de dados de difícil extração de informações.

Esses testes consistem nas técnicas de degradação, em que são proporcionadas simulações controladas das "imperfeições" das imagens no mundo real: como o borramento, variações de luminosidade e ruído; cujo objetivo é identificar como os modelos de aprendizagem profunda reagem a essas adversidades e em que ponto a acurácia do resultado do reconhecimento facial é impactada (Da Silva Moraes, 2023).

Algumas das técnicas mais comuns utilizam as degradações para manipular as imagens a fim de reduzir suas qualidades, nitidez e informações visuais: um exemplo é o redimensionamento, em que a imagem é reduzida de tamanho ao ponto de impactar na extração das informações que representam imagem; outro exemplo é o desfoque, cujo objetivo é simular imagens capturadas em movimento, resultando em uma imagem borrada e com linhas alongadas (Da Silva Moraes, 2023).

Com vistas a mapear o desempenho dos principais modelos de reconhecimento facial disponibilizados, combinados com os três algoritmos de detecção mais utilizados (*dlib, mtcnn, retinaface*), Da Silva Morais (2023) submeteu esses modelos a uma série de testes de degradações. No projeto, utilizou-se o banco de imagens *Labeled Faces in the Wild* (LFW), cuja escolha justificou-se por ser uma base de dados amplamente utilizada para avaliar e montar algoritmos, tendo em vista que contém uma ampla diversidade de poses, expressões faciais, iluminação, apesar de conter baixa diversificação em termos de gênero e etnia. Ao aplicar cada um dos modelos de reconhecimento facial, combinado com um dos algoritmos de detecção, às imagens do banco de imagens com e sem as técnicas de degradação, a diferença de desempenho dos modelos foi alarmante. Destacou-se que o modelo *FaceNet*, desenvolvido pelo Google, quando associado com o algoritmo de detecção *dlib*, obteve o pior desempenho na comparação entre a imagem original e a imagem submetida à degradação máxima de redimensionamento: acurácia de 0.000, enquanto o modelo *DeepFace,* desenvolvido pelo Facebook, obteve, com o mesmo algoritmo de detecção, acurácia de 0.147.

> "(...) Essas percepções destacam a importância de considerar as condições reais de aplicação e os tipos de degradações que podem ser encontrados em ambientes práticos ao projetar sistemas de reconhecimento facial robustos e precisos. Além disso, é fundamental selecionar modelos adequados para cada contexto específico, considerando suas características e comportamento diante de diferentes cenários de degradação" (Da Silva Moraes, 2023, p. 35).

Ante a discrepância do desempenho dos diversos sistemas de reconhecimento facial, em situações que buscam simular a sua atuação na realidade, resta o questionamento de quais são as "combinações" utilizadas nos espaços públicos.

Ponderações sobre o nível de preparo e acurácia dos sistemas incorporados à vigilância lançam dúvidas quanto ao desempenho desses sistemas. Os modelos utilizados nas ruas, combinados com os algoritmos de detecção de imagens, estão preparados para extrair dados de pessoas em movimento ou à distância? Antes de responder esses questionamentos, é importante destacar que tais sistemas podem já ser programados, desde a sua origem, para reagir com eficiência aos efeitos da degradação.

Desde a fase de elaboração do conjunto de treinamento do sistema de reconhecimento facial, os dados de treinamento devem ser pensados visando a representação de novos casos, tendo em vista que "o que se ensina à máquina é o que se espera que aprenda" (Brandão, 2023, p.32). Em outros termos, se nas fases iniciais de montagem da rede neural não forem utilizados dados com variáveis condições, como borramento, baixa luminosidade e desfoque, o sistema não vai ser capaz de sequer identificar tais imagens "degradadas" como fonte de dados e delas extrair os vetores básicos para realizar a submissão da imagem ao processo de reconhecimento facial. Nesse sentido, um rosto borrado pode não ser considerado como uma face, caso o sistema não tenha sido treinado a identificar e buscar informações nesse tipo de imagem. Os dados de treinamento devem refletir uma correspondência com os dados que serão futuramente apresentados ao sistema, as amostras precisam ser representativas (Brandão, 2023).

Nesse raciocínio, um sistema pode apresentar falhas quando seus operadores não buscam incluir um banco de imagens diversificado para compor a fase de treinamento do sistema, ou que não sejam munidos de algoritmos de identificação aptos a identificar rostos em contextos variáveis. Em outros termos, o pleno desempenho da ferramenta é vinculado ao que se espera que ela identifique e classifique. Basta relembrar que o modelo de reconhecimento facial FaceNet está disponível no mercado, ainda que seu desempenho seja péssimo quando a imagem é submetida ao redimensionamento.

Em suma, a composição do sistema de reconhecimento facial consiste em um processo de escolhas:

a) Primeiro, ao selecionar a base de dados de treinamento;
b) Seleção do algoritmo de detecção de rostos;
c) Opção por descartar as etapas anteriores e utilizar algum pré-modelo;
d) Definição do algoritmo fundamental;
e) Ajustes da função estatística de cada nó;
f) Definição de rótulos para os exemplares;

g) Controle na admissão das imagens que contenham dados relevantes e descarte das que só apresentam ruídos.

Ou seja, o sistema de reconhecimento facial é estruturado nas decisões de seus operadores.

Essas decisões devem ser informadas aos consumidores e estados que adquirirem tais sistemas, a fim de que se proporcione a devida transparência quanto à eficiência e *modus operandi* do produto. Todavia, os casos abordados ao longo deste projeto revelam que muitas vezes os estados adquirem essa tecnologia sem informações mínimas e, pior, não buscam mecanismos para averiguar a sua eficiência. Um exemplo foi a contratação realizada no Estádio Centenário, em que as únicas informações disponibilizadas dizem respeito ao que se esperava do desempenho da tecnologia na contratação e aos discursos tecnosolucionistas.

3.1.2. Imprecisões e intersecções raciais e de gênero

Os algoritmos de detecção, essa porta de entrada para a rede neural, não estão somente sujeitos às adversidades das imagens degradadas. Às vezes, uma imagem em perfeito estado pode ser classificada na camada oculta como “ruído” e “barrada” na camada de entrada. O experimento realizado por Joy Buolamwini (2023) chama a atenção para as barreiras cotidianas criadas para as imagens dos rostos “invisíveis” para o sistema de reconhecimento facial.

A pesquisadora do MIT conta que estava trabalhando em um projeto de reconhecimento de imagens e decidiu usar, por questões de praticidade e economia, um modelo pré-pronto, com base de dados e algoritmo de detecção já modelados, cabendo-lhe articular o algoritmo fundamental e ajustá-lo às somas dos nós da rede neural. Quando o projeto estava finalizado, decidiu testar em si, mas, apesar da qualidade da *webcam* utilizada, o seu rosto não foi detectado. Questionando-se se o projeto seria capaz de funcionar em qualquer rosto, buscou o apoio de suas colegas que, prontamente, responderam que o projeto era divertido e que seus rostos foram detectados. Joy estava intrigada com o funcionamento do projeto e resolveu desenhar em sua mão um “L”, linhas horizontais para os olhos e um “U” para o sorriso, simulando assim um esboço de um rosto: o sistema detectou a face caricata. O problema ainda lhe intrigava, por fim resolveu fazer um último teste: colocou uma máscara branca que tinha usado em uma festa fantasia na noite anterior. O sistema reconheceu a máscara branca. A pergunta que persistia era o “porquê” de seu rosto não ser detectado.

Quanto ao experimento, algumas considerações devem ser apontadas, mas a primeira que salta aos olhos diz respeito ao desenho. Ao passar pela camada de entrada, o algoritmo de detecção descartou sua imagem na camada oculta, todavia, não exitou em admitir na rede neural um desenho formado por letras, simplificando elementos atribuídos ao rosto, uma máscara e às colegas de Joy. Outra questão, a pesquisadora só foi capaz de desfrutar do projeto quando utilizou uma máscara branca.

Com base nesse experimento, Buolamwini (2023) articulou o termo "coded gaze", que descreve o olhar computacional para aquilo que deve ser priorizado, ainda que sejam refletidas discriminações no efeito de "apagamento" do irrelevante. O rosto de Joy foi apagado por ser considerado relevante e merecedor de atenção, devido ao fato da pesquisadora ser uma mulher negra.

Desse modo, o olhar da máquina reflete o racismo e o sexismo, ao ponto desses elementos discriminatórios fazerem parte de sua própria composição. E tal constatação não é atual, pelo contrário, esse apontamento reflete uma prática antiga no ramo da edição e detecção de imagens: como no caso das câmeras analógicas, em que estas eram equipadas com filmes compostos por composições químicas destinadas a realçar as "cores desejadas", tais cores tinham como molde uma modelo de pele branca; resultado, a câmera foi ao mercado, sendo bem recepcionada pelo público consumidor, sem que, contudo, demonstrasse aptidão para registrar as pessoas de pele negra (Buolamwini, 2023).

A pesquisadora ainda relata os comentários que recebeu em sua entrevista ao programa TEDx Talks. Ao relatar o mesmo exemplo do filme fotográfico, os comentários ao vídeo indicaram que ela não compreendia as leis da física e que a pele branca apresentaria melhor absorção e reflexão de luz (Buolamwini, 2023). Esses comentários em defesa da máquina fizeram com que a pesquisadora refletisse quanto à interação entre vieses e senso comum no processo de formatação das tecnologias, sejam analógicas ou digitais: "A razão de seu rosto não ser detectado não seria em função de uma falta de contraste baseada na complexidade negra? Ou seja, os algoritmos não são racistas, sua pele que é muito negra" (Buolamwini, 2023, p. 41-42)[2]. A neutralidade das câmeras é posta em cheque, principalmente quando se investiga a sua composição, seja por meio dos produtos químicos e da intenção por trás do uso deles, ou dos modelos utilizados para treinar o "olhar" da máquina.

[2] Tradução livre de: "Isn't the reason your face was not detected due to a lack of contrast given your dark complexion? (In other words, algorithms aren't racist—your skin is just too dark. (Boulamwini, 2023, p. 41-42)".

No caso dos sistemas de reconhecimento facial, o "olhar da máquina" fica ainda mais evidente. A seletividade do "relevante" e "apagamento" da informação indesejável são processos definidos desde a escolha de quais dados irão compor o banco de imagens de treinamento e o de testes: ao incluir no sistema tais dados, o algoritmo de detecção de imagens reconhece que essas informações e suas semelhantes são pertinentes ao sistema. Ou seja, o sistema pré-modelado utilizado por Buolamwini entendeu que o seu rosto não deveria ser admitido na rede neural, ao passo que a caricatura e a face de sua colega branca, sim.

Os exemplares, *samples*, disponibilizados como banco de dados ou de testes, também refletem o poder de quem tem o direito de fala e de ser apresentado: ao contratar celebridades e utilizar imagens disponibilizadas na *internet*, a Amazon proporciona um banco de imagens que espelha as presunções da sociedade, os reflexos de poder (Buolamwini, 2023). A coleta desses dados busca a facilidade, de modo que se opta por buscar imagens de figuras públicas, majoritariamente representadas por homens brancos em posição de poder e modelos estereotipados: essa "naturalidade" na escolha das imagens acaba por reforçar o patriarcado e a branquitude (Buolamwini, 2023). Basta lembrar quem pode usufruir dos privilégios do projeto desenvolvido por Joy, seus colegas brancos.

Nesse sentido, a seleção das imagens abre o leque das possibilidades a serem admitidas no sistema, enquanto fecha as portas para as imagens "desviantes". Nesse sistema de classificação, os algoritmos são os "árbitros da verdade", seja ao admitir no sistema ou atribuir rótulos para as informações: tais mecanismos exercitam o poder de decisão ao modificar, selecionar ou expandir as classificações dos exemplares, são, assim, reflexos de escolhas subjetivas (Buolamwini, 2023). O exemplo clássico, quando os operadores do sistema optam por usar a classificação binária de gênero, masculino e feminino, exclui-se do sistema todas as outras manifestações de gênero, como a transexualidade, e esses rótulos acabam sendo reconhecidos pelo sistema como a "única verdade" (Buolamwini, 2023).

Contudo, o olhar programado e reforçado pelos algoritmos vai além, não basta invisibilizar uma parcela dos dados, também é preciso priorizar os níveis de desempenho da rede neural a fim de não sobrecarregar o sistema. Na (re)definição de prioridades, alguns dados passam por "atalhos" na rede neural, pois assim as múltiplas camadas ocultas direcionam tais dados o quanto antes para a camada final. Quanto mais rápido esses dados são processados, mais tempo sobra para processar os demais.

Um exemplo que ajuda a compreender os impactos desse processamento às pressas é abordado por Buolamwini no seu livro (2023). A pesquisadora relata que, após ter ficado intrigada com a composição do banco de imagens da Amazon, decidiu buscar a formação dos dados utilizados pela NIST (National Institute of Standards and Technology), vinculada ao departamento de comércio estadunidense. O relatório obtido foi surpreendente, pois, ao avaliar a composição do conjunto de dados, detectou que os homens brancos representavam 59.4% do conjunto, ao passo que as mulheres negras sequer chegaram aos 5%: o sistema foi considerado eficiente, pois, ainda que falhasse em todos os casos envolvendo mulheres negras, a sua eficácia ainda seria de 95.6% (Buolamwini, 2023).

Em suma, o "olhar da máquina" precisa ser educado. Num processo de aprendizagem, esse olhar decora os modelos e exercita o seu algoritmo com os exemplos, tudo isso, sob supervisão do programador. Pois foi esse que selecionou o seu "material didático", com o código de computador, estabeleceu-se o padrão, o rótulo dos binômios certo/errado, relevante/descartável. Com esse olhar, o sistema é capaz de aprender e reproduzir padrões de prioridade, ao calibrar os valores desejáveis para a soma estatística de seus nós: estatística em razão da imprecisão do resultado, o "certo" pode estar entre 30-55% de chance de êxito e, no final da corrida pela rede neural, a camada de saída vai ser um conjunto de chances de acerto.

Essa máquina neutra e precisa opera facilmente em um cenário de miopia. Sem enxergar os rostos à distância, diz ser capaz de extrair seus dados principais e de classificá-los, ainda que seus algoritmos de detecção sejam falhos. A mesma máquina ainda é capaz de decidir quando não enxergar. Em sua programação, uma caricatura pode ter mais relevância do que um rosto de uma mulher negra. Um sistema que se diz livre de vieses, ao passo que é estruturado por eles. Todavia, essa ferramenta está disponível no mercado, pronta para imediato consumo, a razão é simples, não possui falhas.

3.1.3. Quando os operadores do sistema decidem ignorar a falha

Quando uma ferramenta de reconhecimento facial é lançada no mercado com índices de acerto de 95.6%, o seu *software* é tido como bem-sucedido e eficiente, ainda que no processo sejam apresentadas taxas de erro para um grupo sub-representado no conjunto de treinamento. Os outros 4.4% de índices de erro são vistos como falhas eventuais, números de menor importância.

O mesmo argumento ainda pode ser observado quando a "cifra do erro" aumenta para 46.8% em sistemas montados por gigantes no mercado como a IBM: a empresa expôs à venda um produto com uma das maiores disparidades já identificadas na acurácia dos produtos que usam IA (Buolamwini, 2023). Ambos os sistemas possuem um ponto em comum, a "falha" diz respeito ao uso do software de reconhecimento facial em mulheres negras. Esses índices de "falha" foram classificados como irrelevantes.

Tais exemplos não são pontuais, tampouco desconexos da realidade em que tais ferramentas foram aplicadas. São casos cotidianos e que atingem grupos específicos, populações que não tiveram lugar no jogo de interesses do olhar da máquina. Esses casos, por mais numerosos que sejam, são considerados eventuais e meros "erros de desempenho", ou seja, como vicissitudes que podem ser corrigidas.

Ocorre que tais falhas já estão presentes no modelo de fábrica dos algoritmos de reconhecimento e banco de dados de treinamento. Ou seja, as falhas não são descobertas, elas sempre estiveram lá: tais falhas são "agregados sociotécnicos" formados por modelos matemáticos, classificações e valores pessoais, tudo isso, escrito nos códigos de programação (Edler Duarte, 2024). Nesse sentido, "erro" pode assumir várias roupagens e justificativas:

> "(...) O erro em determinada tecnologia de segurança decorre de incentivos institucionais questionáveis? Ele deriva da ação de profissionais corruptos? É fruto de uma cultura de inovação que privilegia impermanência e otimização? Surge como resultado de problemas estatísticos causados pela negligência sobre vieses de origem e "feedback loops"? Dependendo de como respondemos a essas perguntas, distribuímos também as responsabilidades, desenhamos as alternativas de intervenção e apontamos para um horizonte político sobre consequências aceitáveis ou não da inovação tecnológica. Desse modo, a forma pela qual definimos o erro guia nossa ação, seja em prol de mais um techno-fix (Morozov, 2013) ou de uma crítica abrangente às práticas de segurança" (Edler Duarte, 2024, p.12).

Ademais, os erros apontam para a subjetividade da máquina, ou, ao menos, de seus programadores. Quando é decidido o nível de prioridade e estabelece-se que o sistema precisa fazer uso das camadas ocultas para selecionar e classificar o quanto antes alguns dados, os algoritmos decidem que tais informações não são merecedoras de atenção. As falhas pendem para um lado da balança, elas não são distribuídas. Afinal, "o que a acurácia não revela sobre as questões em torno do fracasso? Quando o sistema falha, como estão distribuídos os erros? Não devemos assumir uma distribuição igualitária" (Boulamwini, 2023, p. 132)[3].

[3] Tradução livre de: "What accuracy doesn't reveal are questions around failure? When a system fails, how are the errors distributed? We should not assume equal distribution of errors"(Boulamwini, 2023, p. 132).

Os exemplos abordados ao longo do texto indicam que, debaixo do véu da cifra da falha, há a branquidade e o patriarcado, em que a distribuição dos erros é certeira aos grupos selecionados como “de menor importância”.

Os custos de manter essa “cifra de erro” não se resumem às falhas de desempenho na classificação de algumas imagens. O julgamento incorreto feito pelo algoritmo pode ter impactos no mundo concreto. Um exemplo que ilustra bem os “custos da exclusão” está relacionado ao campo da saúde oncológica, mais especificamente à detecção de indícios cancerígenos por meio de um algoritmo que faz a leitura dos dados da pele dos pacientes: ao analisar os resultados, constatou-se que tal exame era voltado para os pacientes com peles “claras” (Boulamwini, 2023). Tais pacientes puderam usufruir do privilégio de ter o câncer detectado nas fases iniciais, enquanto os pacientes negros não tiveram a mesma sorte.

Todavia, a discussão quanto aos privilégios de participar do banco de dados tem um contraponto. Nos “custos da inclusão”, a sobrerepresentação de certos grupos no conjunto de dados de treinamento pode impactar nos valores das somas dos nós da rede neural. Alguns dados podem apontar para presunções tão fortes que já são encaminhados para a rotulagem da camada final. Há dados cujo rótulo é detectado logo pelo algoritmo de reconhecimento.

Algumas ferramentas destacam ainda mais o “peso” das presunções iniciais sobre os dados. Um exemplo são os sistemas ofertados no mercado. Um grupo de pesquisadores utilizou o *software* desenvolvido pela Amazon para verificar o reconhecimento facial na detecção de suspeitos: as fotos apresentadas ao sistema foram as de membros do Congresso Americano e o resultado revelou que, apesar de as pessoas de cor comporem apenas 20% do corpo legislativo, esse grupo teve quase o dobro de falsos negativos (Snow, 2018). Em outros termos, quando o aplicativo falhou ao indicar um parlamentar como criminoso, em 40% dos casos ele era negro.

Com uma ferramenta capaz de classificar, discriminatoriamente, as pessoas como suspeitas, a sua aplicação na segurança pública desencadearia um efeito de contenção em massa de grupos já estigmatizados. Como uma das principais fontes de dados para os relatórios da segurança pública, os impactos do “tirocínio” policial não devem ser subestimados: De Deus Garcia aponta que esse tipo de tecnologia, sob a roupagem da legalidade, tende a repetir e justificar os vieses da atuação policial sobre os grupos marginalizados (2021, p. 16).

Com uma espécie de “faro” para o crime, a atuação policial toma a intuição, advinda da experiência e do aprendizado nas ruas, como base para justificar as suas abordagens (Duarte; Muraru, et al. 2014).

Nesse raciocínio, Duarte descreve o processo de seleção de suspeitos na atuação policial, indo desde quais tipos de denúncia serão atendidas aos "elementos" que passarão pelas revistas. Um processo que é altamente discriminatório em sua gênese, performance e justificação dos resultados:

> "Neste contexto, padrões de seletividade racial poderiam resultar da conjunção de fatores, aparentemente externos ao policial, como, por exemplo, a denúncia anônima, o que pode servir para excluir a assunção, por parte do policial, de que estaria efetuando uma atividade discriminatória. **Não obstante, a decisão de abordar reflete os conhecimentos transmitidos institucionalmente sobre quem são os suspeitos "adequados"**. Esse padrão que, aparentemente, resulta do modo como se estabelece o fluxo de informações, sem possibilidade de um debate sobre a sua validade, serve a um só tempo para garantir a permanência de resultados seletivos e isentar os agentes pelas seleções efetuadas" (DUARTE;MURARU, et al. 2014, p. 91, grifo nosso).

Ante o questionamento da composição dos dados, o exemplo do experimento feito com a ferramenta disponibilizada no mercado pela Amazon ganha um *background*. O resultado na atribuição dos rótulos de "suspeito criminal" à parcela correspondente dos senadores negros é sintoma do conjunto de banco de dados e das decisões tomadas pelos algoritmos nas camadas ocultas. As somas relativas aos vetores extraídos das imagens desses parlamentares possuem maior impacto: a presunção inerente ao dado lhe abre um atalho através da rede neural e o conduz mais facilmente à camada de saída.

Esses processos decisórios, que se dizem neutros, são estruturados por decisões de seus operadores, seja ao utilizar o "faro" policial para aproveitar os rótulos atribuídos ao banco de imagens do grupo dos "suspeitos criminais" ou na forma como tais decisões são mantidas. A função matemática do algoritmo fundamental é formada por subjetividades, ao passo que as replica em larga escala.

Desse modo, o uso dessas ferramentas no sistema de segurança pública deve ser observado com cautela, principalmente quando lhes é apontado um holofote, enquanto as mesmas são anunciadas como "solução" à escalada da violência. O tecnosolucionismo dos "modernos" sistemas de vigilância esconde um dos propósitos desse mesmo sistema: a perpetuação da seletividade do aparato de vigilância criminal:

> "O ponto central, portanto, pode ser sintetizado da seguinte maneira: se os dados que alimentam as bases são coletados e produzidos mediante instituições policiais que levam em consideração e replicam estigmas criminais ligados à raça, por exemplo, as decisões sugeridas mediante o processamento e cruzamento de dados reproduzirão esses vieses, que serão usados para intensificar a atuação seletiva das forças governamentais nesse sentido, num ciclo vicioso" (DE DEUS GARCIA; BONTEMPO CÂNDIDO GONTIJO, 2021,p. 30).

É necessário romper esse movimento cíclico de reprodução dos estigmas nos conjuntos de dados e a consequente classificação de novos dados com fundamentos enviesados. E, para atingir esse fim, faz-se imperativo (re)discutir a ontologia da "falha", sua razão de ser e motivos de se perpetuar. Os debates não podem se resumir aos apontamentos de eventuais "desvios" e "imperfeições do sistema, mas sim entender a razão por trás da frequência e repetição desses "erros".

A "ignorância estratégica" também merece destaque nos debates das inovações no campo da segurança pública: a "repolitização" da falha deve ter como foco os limites do "tecnodeterminismo"; na porosidade do sistema de segurança pública, ao explorar as "frestas" abertas pela presumida margem de erro; e, por fim, a análise do "erro" como um resultado das relações de poder (Edler Duarte, 2024) e espaço de disputa de seus efeitos.

4. O COMPROMISSO DAS EMPRESAS FORNECEDORAS

Em 2019, a principal empresa que atua na Argentina e no Brasil, a NEC, teve seu algoritmo usado em um caso de prisão injusta nos EUA: e, apesar de comprovado que houve o uso de dados enviesados no carregamento do sistema, a provedora não manifestou empenho em evitar situações semelhantes (Access Now, 2021).

Os casos de erros na identificação de suspeitos criminais não são isolados, pelo contrário, eles marcam presença no noticiário da América Latina. Ainda em 2019, um cidadão argentino foi confundido com um suspeito criminal e passou 6 dias detido: a aparência e nome em nada eram parecidos com o do foragido, apesar da alegada taxa de erro de apenas 3% da TRF utilizada (Hayon, 2019). Em entrevista, a autoridade executiva responsável pela implementação da ferramenta argumentou que a situação foi um mero "erro" no sistema da base de dados e, não necessariamente, no do reconhecimento facial (D'Alessandro *in* Hayon, 2019). Contudo, especialistas argumentam que o uso dessa base de dados *per si* já representa um erro, uma vez que as informações não foram devidamente agrupadas, estavam desatualizadas e chegou-se ao ponto do algoritmo apontar como infratores indivíduos de causas que já prescreveram há anos (Cabello, *in* Hayon, 2019).

Com regramentos esparsos, ausência de base jurídica específica e definições genéricas, essas regiões mostram maior interesse em incorporar a referida tecnologia do que em adequar seu uso aos direitos dos cidadãos (Venturini; Garay, 2021). É um uso que, conforme já descrito anteriormente, caracteriza-se pelos elevados índices de imprecisão, quando diante de uma base de dados "contaminada" pelos vieses dos operadores do algoritmo.

Evidente, pois, a necessidade de cautela para com o manuseio desse tipo de tecnologia, entretanto, alguns países a incorporaram sem o preparo mínimo.

A situação agrava-se quando se leva em conta que no Brasil e Uruguai há regulamentos para a proteção de dados pessoais que expressamente excluem a sua incidência nos casos do uso de dados para fins de segurança pública: a repressão da criminalidade dispensaria o cumprimento do princípio da privacidade e do dever de proteção dos dados pessoais (Abbas da Silva et al., 2020).

Nesse sentido, os próximos capítulos serão dedicados à análise de caso do processo e contexto de contratação das tecnologias de reconhecimento facial no âmbito da segurança pública do Uruguai e Brasil.

4.1. As câmeras e o futebol uruguaio

Em 2022, um jogador do clube uruguaio Peñarol foi atuado em flagrante nos arredores do estádio em que seriam celebradas as finais, o motivo, porte ilegal de uma pistola e de oito projéteis: em entrevista à imprensa, a promotora responsável por oferecer a denúncia informou que o jogador já vinha sendo investigado há um tempo, inclusive, apontou-se que ele seria responsável por fornecer armas aos membros dos *barras bravas* e pichar os muros da cidade junto dos integrantes dessas torcidas violentas (ORTEGA, 2022).

Quanto aos muros, esses atuam como os registros de posse das ruas *barras.* Disputas pelos muros são comuns na cidade de Montevidéu, inclusive com incidentes envolvendo disparos com armas de fogo e ataque aos membros de torcidas rivais (ORTEGA, 2022).

Entretanto, os muros e o mercado de armas representam apenas parte das empreitadas das torcidas violentas. Os *barras bravas* também possuem posição de destaque no controle do narcotráfico uruguaio. Em 2015, as duas principais gangues que chefiavam o tráfico de drogas na zona das 40 semanas em Montevidéu entraram em embate: no confronto, um dos "cabeças" do crime e chefe dos *barras bravas* do clube Peñarol foi assassinado pelo rival. O homicídio resultou em uma guerra entre as gangues que perdurou ao longo de três anos (Scognamiglio, 2024). O leque de atuação dos *barras* é amplo e as arquibancadas são sua casa.

A presença massiva de gangues violentas nos estádios tem preocupado a *Asociación Uruguaya de Fútbol (AUF)*. Em comunicado à imprensa, a AUF, que inicialmente havia adotado postura colaborativa, destacou que, frente aos "cartéis" liderados pelos *barras,* caberia atuação exclusiva da polícia e da justiça uruguaia lidar com essas "organizações criminosas" (Gagne, 2017). As organizações da sociedade civil e empresas privadas não teriam forças frente ao poderio das torcidas organizadas.

Buscando atender às demandas coletivas por maior segurança nas ruas e arquibancadas, iniciou-se o movimento de tolerância zero aos *barras*. Em 2013, a Lei nº 19.120 alterou o Código Penal para majorar a pena descrita no art. 360 do código: participar de provocação e participação em desordem em espetáculo público, sete a 30 dias de prestação de trabalho comunitário, se não for subsumido ao delito de riña, o qual é punido com três a 24 meses de prisão, conforme o art. 323 bis (Uruguay, 1967).

Como a intimidação da pena abstrata não foi suficiente para afastar as torcidas violentas de cena, foram necessárias novas providências. Em 2016, o Decreto 387/216 buscou atuar nas formas de aquisição e entrada nos estádios.

Dentre as medidas adotadas destacam-se: a formação de um banco de dados com as informações pessoais de quem comprou os ingressos; recomendação para não se admitir aos estádios os torcedores com históricos penais dos delitos dos arts. 360 e 323 *bis* do Código Penal; limitação do número de convites cortesia a serem distribuídos pelos clubes e obrigatoriedade dos dados dos destinatários serem informados ao *Ministerio del Interior*; determinação para imediata instalação de câmeras de reconhecimento facial nos estádios (Uruguay, 2016).

Em 2024, o MI decidiu entrar em campo. Ao criar a figura do Evaluador de Seguridad, buscou-se intensificar a presença do corpo policial nas arquibancadas: o arranjo encontrado é fruto das discussões conjuntas entre a AUF e a Secretaria Nacional de Deporte na reunião que apurava formas de garantir a segurança dos torcedores e árbitros em campo (Montevidéu, 2024). Fez-se necessária a presença de um oficial da polícia no meio da arquibancada para proporcionar maior segurança aos estádios.

Nesse raciocínio, percebe-se uma relação intrínseca entre a criminalidade e a atuação violenta das torcidas organizadas, de modo que, ao mitigar a influência e mapear os seus membros, espera-se que os índices de crimes como tráfico de drogas e homicídios sejam reduzidos. São atores que operam em zonas específicas, como nos arredores dos estádios. Desse modo, a atuação do Ministério del Interior busca atingir a máxima eficiência de Pareto, pois atua como se 80% dos incidentes ocorressem em uma área correspondente a 20% da zona metropolitana de Montevidéu (Fagundez, 2023). Em outros termos, o MI escolheu os *barras* como principais e potenciais alvos do controle. Tais grupos desviantes devem ser monitorados e os dados de seus membros compilados.

Com a “caça” aos membros das torcidas violentas figurando na pauta política, os aparatos de vigilância ganham especial destaque. Os estádios se tornam palco para a estreia da moderna tecnologia de reconhecimento facial e vitrine para espelhar o horizonte da segurança, uma miragem a ser alcançada nas ruas. As ferramentas de vigilância são expostas nas arquibancadas como produtos e incentivam os departamentos de polícia das variadas regiões a consumir tais tecnologias.

4.1.1. Estádios como vitrine

Enquanto as novas tecnologias de vigilância ainda não são utilizadas de modo efetivo nas ruas, os experimentos realizados nos estádios de futebol ajudam a proporcionar o perfil operacional do uso dos sistemas de reconhecimento facial na segurança pública.

O uso dessas ferramentas nos estádios e shoppings passa a servir de parâmetro para a polícia (Fernández, 2022). E, no caso do Estádio Centenário, o uso das ferramentas de tecnologia se mostrou efetiva na redução dos índices de incidentes violentos, ao ponto de "transformar'' a experiência nos estádios (Fernández, 2022).

A presença e o uso das câmeras de monitoramento nas arquibancadas são vistos como fatores determinantes no aumento da percepção de segurança pelos torcedores e frequentadores do estádio. Os argumentos do *Ministerio del Interior* servem como um reforço à propaganda do sistema HERTA utilizado nos estádios. O MI divulgou que, graças ao uso das câmeras, os incidentes violentos nos estádios caíram em 90% e que, ao longo de seus cinco anos de uso, tal sistema, em conjunto com as ferramentas utilizadas nos outros estádios, foi essencial para levar a violência nos estádios ao fim (Fernández, 2022).

Apesar de os resultados divulgados pelo MI serem controversos, ainda mais quando confrontados com a constância dos índices elevados de agressões aos árbitros e com o fato de ter sido necessária a presença de um oficial da polícia nas arquibancadas, a experiência dos estádios é tida como modelo exemplar para o uso das tecnologias de segurança.

Aproveitando o bem-sucedido *software* de reconhecimento facial, o próximo passo é expandir a área de atuação dessa ferramenta. Nesse sentido, o MI tem empreendido esforços para equipar a capital uruguaia com a presença das câmeras: de 2010 até 2022, foram adquiridas mais de 8.433 câmeras filmadoras, que variam entre os modelos que rotacionam 360º, ferramentas com reconhecimento de caracteres e as equipadas com reconhecimento facial (Fernández, 2022). Com o MI assumindo a vanguarda da "modernização", a polícia não pode ficar para trás, pois *"en cuanto al rol que debe cumplir la Policía Nacional, podemos afirmar que la incorporación de nuevas tecnologías puede aportar significativamente a la compleja tarea de mejorar la Seguridad Pública"* (Fernández, 2022, p. 41). Manter-se atualizada com as novas tecnologias de vídeo monitoramento passa a ser um dever da polícia.

A Polícia Nacional deve continuar empenhada no combate à criminalidade, devendo acompanhar as evoluções da sociedade e suas novas nuances, ao ponto de ter de manter-se sempre na dianteira em termos de capacitação de seu corpo funcional e equipada com novas e eficazes ferramentas (Fernández, 2022).

Assim, como os discursos apontaram que a presença das câmeras foi decisiva para o aumento na percepção de uma melhora na segurança nas arquibancadas, tais argumentos também buscam a mesma tendência nas ruas. Esse esforço de constante busca por aprimoramento é bem-vindo.

O uso das câmeras de monitoramento nas ruas é essencial ao poder contribuir positivamente para a imagem que os cidadãos têm da polícia, segundo o Diretor de Criminalística da Direção Nacional da Polícia Científica uruguaia, Comissário Major Robert García Fernández (2022). Além disso, o Comissário também destaca a imprescindibilidade das câmeras de reconhecimento facial para formação do conjunto probatório no processo penal, principalmente quando aliadas às demais tecnologias de investigação criminal, como o perfil genético e a identificação das pupilas.

"Modernizar" o instrumental utilizado no trabalho de investigação é visto como sinônimo de redução de trabalhos desnecessários e de melhor alocação de recursos humanos (Fagundez, 2023): ou seja, o investimento na tecnologia é compensado por sua eficiência, principalmente quando aliado ao aproveitamento do material proporcionado pela polícia. O encarregado da Divisão de Sistemas de Informação do Ministério do Interior, Comissário Geral Fabrício Fagundez (2023), defende que o uso das novas tecnologias de vigilância deve ser alicerçado na vasta experiência do corpo policial. Experiência essa que conta com um banco de dados que varia entre informações de sistemas de gestão das ruas e emergências às informações coletadas pelos patrulheiros em policiamento de rotina (Fagundez, 2023).

No bojo de sua argumentação, o Comissário Geral defendeu o uso de algoritmos de predição de delitos, como forma de agregar ao trabalho de prevenção de delitos maior eficiência, precisão e economia de tempo:

> "Los delitos, por naturaleza son un fenómeno intrínsecamente aleatorio, por lo que no es posible hacer una predicción perfecta de ellos, pero mediante modelos matemáticos y el uso de algoritmos, se maximiza la probabilidad de identificar donde ocurrirán" (Fagundez, 2023, p. 53)

Adotar o quanto antes as novas tecnologias de vigilância passou a ser tido como um imperativo. O Uruguai conferiu especial destaque, em seus planejamentos de gestão estratégica da máquina pública, ao fomento e uso de IA nas diversas esferas do governo, dentre elas a segurança pública (Fagundez, 2023). A "modernização" é tida como uma meta a ser cumprida para se fortalecer a cidadania e, na corrida para cumprir as metas, o Ministerio del Interior tem assumido a vanguarda.

4.1.2. O Protagonismo do Ministerio del Interior

Ante o exposto pelos dois comissários, resta nítido que, em termos de modernização da segurança pública, a figura do *Ministerio del Interior* se destaca. Sua competência administrativa é ampla, indo desde a preservação da paz e redação das políticas de segurança dentro do território nacional até a coordenação da Polícia Nacional (Sanjurjo; Trajtenberg, 2022). É um órgão de direção, ao passo que sua influência se encontra capilarizada, principalmente nos departamentos de polícia das metrópoles uruguaias.

Atuando desde o acompanhamento do processo de aquisição de sistemas de reconhecimento facial e monitoramento dos estádios até a aquisição de novas câmeras de vigilância para as ruas, o MI se faz presente tanto no âmbito público quanto no privado. E, dentro das recentes políticas do Ministério, merece especial destaque o seu investimento no uso de protótipos de IA. Com o uso de uma tecnologia israelense, o MI pretende que Montevideu faça parte do plano-piloto de testes de uma ferramenta de vigilância capaz de identificar atitudes "suspeitas": no projeto inicial, a máquina usará em seu banco de dados as condutas atribuídas como "suspeitas" para detectar em tempo real atitudes similares e alertar aos oficiais de plantão (Subrayando, 2023).

Em sua fala, o *Ministro del Interior*, Luis Alberto Heber, destacou a oportunidade de aprendizado conjunto, entre o software que precisa ser "ensinado" e o operador que passa a compreender e construir as possibilidades de se prevenir o delito (Subrayando, 2023). Por fim, Heber destacou os benefícios que tais ferramentas trariam para aumentar a segurança dos cidadãos:

> "Estamos trabajando, entendemos la preocupación. Yo también estoy preocupado. Con estas herramientas (cámaras) podemos protegerlos. Nosotros no podemos resolver todos los problemas en cinco años pero venimos bajando (los delitos)" (Heber, 2023 *in* SUBRAYANDO, 2023).

Nesse sentido, a experiência policial iria servir de insumo básico para o funcionamento da ferramenta de monitoramento, fornecendo, assim, os rótulos necessários para os algoritmos fazerem as classificações das imagens detectadas, seja ao final da rede neural ou em alguma camada oculta. O faro policial, munido de toda a sua subjetividade, passa a estruturar o banco de dados do *software* e integrará o resultado neutro da classificação algorítmica dos suspeitos.

Para além das novas empreitadas tecnológicas do MI, um fator que merece especial destaque é o seu vasto sistema de compartilhamento de dados. Com os investimentos ao longo dos anos na integralização das informações armazenadas no Sistema de Gestão de Segurança Pública, a rede de dados passa a contar com registros de delitos e acidentes, bem como com os dados pessoais das pessoas envolvidas nesses ocorridos: informações como registro de veículos, porte de arma, geolocalização, registro de empresas e reservas em hospedagens e pensões (SGSP, 2020). Essa teia de dados, sob o comando e direção do MI, permite que seja traçado o perfil completo dos cidadãos envolvidos em acidentes e em delitos.

Entretanto, o tamanho do leque de atuação e o envolvimento do Ministério podem trazer complicações operacionais nas atividades de rotina. O *Ministerio del Interior*, como órgão de cúpula e formulador das políticas públicas da Segurança Nacional, deveria ser encarregado das funções relacionadas à elaboração e avaliação das políticas de segurança e não envolver-se na execução direta dessas políticas (Gonçalves Feliz; Duarte, 2024). Em outros termos, cabe ao MI, como órgão decisório, indicar as metas a serem cumpridas, cabendo aos departamentos regionais de polícia o desenvolvimento dos pormenores dos projetos e das etapas de sua aplicação. Contudo, o que se observa é que essas competências são absorvidas pelo MI.

Essa divisão de tarefas, entre os órgãos de cúpula e os departamentos regionais, dá-se em razão da qualidade e adequação do serviço prestado. Os encarregados de executar as políticas públicas possuem contato direto com o contexto em que elas serão aplicadas e não sofrem pressões externas como os órgãos responsáveis pelo processo decisório:

> "O longo mandato dos gestores públicos no setor público, por exemplo, ajuda não só a manter a atenção em questões de políticas públicas específicas, **mas também lhes permite ter uma perspectiva de longo prazo sobre a política pública, condições que os dirigentes políticos, enfrentando pressões eleitorais e outras de curto prazo, muitas vezes não têm. Em comparação, os formuladores de políticas públicas no nível superior, como ministros, legisladores e governadores, enfrentam prazos muito mais curtos no cargo e têm proporcionalmente mais dificuldade em influenciar a direção e o conteúdo da criação de políticas em longo prazo**. A segurança e experiência no trabalho desfrutadas por gestores públicos, especialmente servidores públicos de carreira, também os protegem de pressões políticas (como a necessidade de ganhar as eleições) que restringem líderes políticos, quando se trata de questões de políticas públicas. Como resultado, os gestores de políticas são capazes de dar tanto uma perspectiva de longo prazo sobre a criação de políticas, como um maior peso às considerações técnicas na elaboração e implementação delas" (WU, 2014, p. 17).

Observa-se que, em se tratando de formulação, execução, monitoramento e avaliação das políticas públicas de segurança pública, o *Ministerio del Interior* assume o protagonismo em todas as etapas da implementação dessas políticas públicas.

Tal movimento ruma na direção contrária ao recomendável e esperado da gestão da máquina pública. Há um descompasso entre o decidido e avaliado de forma positiva pelo mesmo ator e a realidade da implementação dos projetos.

A eficiência na alocação de recursos e a efetividade do resultado entregue e percebido pelos cidadãos são postas em cheque: a política pública acaba por ser desproporcional ao contexto local e os dirigentes regionais não conseguem adequá-la ou monitorá-la, por falta de autonomia no processo de implementação da política pública (Gonçalves Feliz; Duarte, 2024). Todavia, nessa reunião de atividades executadas pelo MI, a eficiência e a qualidade do produto entregue não são os únicos fatores prejudicados, a neutralidade na avaliação e monitoramento dos resultados também são impactadas. As avaliações passam a ser tendenciosas e vagas, como no caso da entrega de resultados do desempenho do sistema de reconhecimento facial no Estádio Centenário.

Quando os índices e relatórios de desempenho são substituídos por comentários genéricos ao bom funcionamento das ferramentas adquiridas, é necessário buscar de forma ativa qualquer informação que diga respeito ao produto final entregue à população. E, no caso das tecnologias de monitoramento, um quadro útil de informações pode ser encontrado nas leis que autorizam e regulam o seu uso, bem como nos sistemas informáticos que acompanham o processo de aquisição das ferramentas de vigilância.

4.1.3. As Formas de Aquisição da Tecnologia

Quanto ao marco normativo que regulamenta as formas de aquisição e uso das ferramentas de tecnologia e vigilância na segurança, um fato chama a atenção: o desamparo.

No Uruguai, as diretrizes, deveres e direitos referentes aos dados pessoais são conferidos pela Lei de Proteção de Dados Pessoais Uruguaia (LPDP), a Lei nº 18.331. Esse marco normativo elenca, desde o seu art. 1º, a proteção de dados pessoais como direito inerente à dignidade da pessoa humana, todavia, reconhece no art. 3º que a Lei não se aplica aos dados coletados e mantidos em bancos de dados para fins de segurança pública e investigação penal (Uruguay, 2008). A proteção constitucional dos dados pessoais perdeu fôlego frente ao imperativo da segurança pública e manutenção da ordem e paz.

Com vistas a eliminar eventuais contradições, a LPDP, em seu art. 25, foi sistemática ao indicar que as bases de dados mantidas pelas Forças Armadas e organismos policiais de inteligência e de antecedentes penais devem ter registro permanente.

O artigo destaca que o tratamento de dados pessoais sem o consentimento de seus titulares somente pode ocorrer em hipóteses restritas, onde seja necessário o cumprimento de missões legalmente reconhecidas de defesa nacional, segurança pública e repressão de delitos: o diploma legal que autorizar esse tratamento deve indicar bases de dados específicas e os dados pessoais eliminados do sistema quando cessarem as averiguações que motivaram a sua inclusão (Uruguay, 2008).

O marco normativo que regula o uso dos dados pessoais para fins de segurança pública é limitado. Um contraponto às autorizações de compras e utilização das tecnologias de monitoramento. Nos estádios, o Decreto nº 1/021, que modifica as condições de ingresso nos estádios, determina que todas as pessoas classificadas na "lista dos impedidos" devem ter a sua imagem incluída no banco de dados do sistema de reconhecimento facial do estádio e que nas partidas consideradas como "de risco" devem ser usadas as ferramentas de reconhecimento facial nas arquibancadas e controle nas entradas dos estádios (Uruguay, 2021).

Essa atuação do MI nos espaços públicos e privados é conferida pelo art. 1º da Lei Orgânica Policial Uruguaia, Lei nº 19.315, em que cabe ao Ministério a manutenção da segurança pública interna (Uruguay, 2015). Munido da autorização genérica imposta por esse artigo, o MI lança o seu poder decisório sobre as ruas e estádios. E, com o sucesso nas arquibancadas, a sua mais nova empreitada é levar o modelo prodígio do reconhecimento facial para as ruas de Montevidéu.

Inicialmente, há um empecilho legal e um problema de congruência técnica nesse esforço por popularizar a capital uruguaia de câmeras. A incongruência técnica diz respeito ao problema fundamental do uso do reconhecimento facial na segurança pública, a base de dados. Buscando fugir de *softwares* genéricos estrangeiros, a polícia uruguaia deve calibrar o algoritmo fundamental da rede neural, ajustar os pesos dos nós e definir os rótulos desejados, para então poder lograr bons resultados na aplicação da ferramenta nas ruas. Para garantir o bom funcionamento dos sistemas de reconhecimento facial e de predição, a vasta experiência compilada nos bancos de dados do Sistema de Gestão de Segurança Pública (SGSP) deve ser utilizada (Fagundez, 2023) como insumo básico.

Ocorre que nem todos os dados dos cidadãos estão nos sistemas de policiamento. Haveria um desfalque na rotulagem das informações, caso o sistema fosse munido apenas com os dados da SGSP. Para garantir a eficiência algorítmica e o monitoramento de todos os transeuntes, o sistema de reconhecimento facial precisava ter acesso aos dados da Direção Nacional de Identificação Civil.

O “empecilho” está na vedação conferida pelo art. 21 da Lei nº 14.762, em que os dados armazenados no sistema são referentes às identificações das pessoas físicas, empresas e empresários e são absolutamente reservados, de modo que lhes é vedado ter outros usos que não previstos em expressa autorização legal (Uruguay, 1978).

Todavia, como as metas do governo uruguaio passam pelo uso de IA em todos os órgãos, o MI não poderia ver freado o seu movimento de modernização da segurança pública. Nesse modo, buscou amparo no Pressuposto Nacional de Gastos Públicos do exercício financeiro de 2020-2024. Esse é um documento elaborado pelo Poder Executivo e aprovado pelo Poder Legislativo: o documento contém a prestação de contas do ano civil anterior, um balanço de execução e seções destinadas aos gastos e estimativa de arrecadação dos exercícios seguintes (Ministerio de Economía y Finanzas, 2020). É um documento de natureza orçamentária, cujos gastos devem ser aprovados pelos membros do corpo legislativo.

Ocorre que no Pressuposto de 2020-2024, foram incluídos artigos que viabilizam a migração dos dados da Direção Nacional de Identificação Civil para o banco de imagens do sistema de reconhecimento facial do *Ministerio del Interior* (Santos de Amores, 2022).

Apesar de os artigos terem sido aprovados e estarem vigentes, cabe destacar os comentários dos membros do Senado na discussão do projeto do Pressuposto. Em menção aos artigos 178, 179 e 182 do documento, a Senadora Nane mostrou-se preocupada com a legalidade e abrangência da autorização expressa nos artigos:

> “Ahora bien, la categorización de decir que lo voy a utilizar con fines de seguridad pública es tan amplia que a nosotros nos parece que deja un flanco abierto al uso indebido, quizá no en un gobierno democrático. **Quiero resaltar que no estoy asignando absolutamente ninguna intencionalidad, sino diciendo que el alcance es demasiado amplio y que poner esto en una ley de presupuesto no habilita un debate social sobre el tema de la vigilancia del Estado, utilizando datos de reconocimiento facial**. Este artículo no habilita ese debate que entendemos es absolutamente fundamental por el uso posterior que puede tener. Consideramos que en este debate tiene que estar incluida la academia, la industria y la sociedad civil.(...) **Las preguntas van en el sentido de qué previsiones de uso futuro podríamos estar tomando en un proyecto de ley de presupuesto porque no se puede reglamentar su uso posterior.** ¿Qué medidas de seguridad vamos a aplicar después a esa base de datos? ¿Cuáles son esos usos específicos de seguridad pública? ¿Tenemos una medición de impacto?” (Nane, 2020 in Asunto 147701, 2020).

Os questionamentos da Senadora não foram respondidos, pelo contrário, foram silenciados com o argumento do Senador Calabria, que comenta que a migração de dados faz-se necessária ante o investimento do Ministério em uma plataforma de reconhecimento facial: *“pero, reitero, ese planteo, esa discusión quizá debió hacerse antes de que el Estado gastara más de USD 1:000.000 en un instrumento. Ahora lo que hay que hacer, en todo caso, es*

utilizarlo, y nosotros lo que estamos haciendo es darle el marco jurídico para eso" (Calabria, 2020 in Asunto 147701, 2020). Em outros termos, o dispendioso projeto do MI precisava ser implementado o quanto antes, para justificar tamanho gasto com os cofres públicos.

Quanto a esse projeto do *Ministerio del Interior* cabem alguns apontamentos, haja vista que, além de ter sido motivo de intensas discussões na aprovação do Pressuposto, tal empreendimento também veio a ser questionado em via judiciária.

4.1.4. ARCE e licitações presentes

Apesar do valor despendido no sistema de reconhecimento facial, exigiu-se demasiado esforço para localizar essa aquisição de um milhão de dólares do MI. Após buscas junto aos sites oficiais do *Ministerio del Interior* e da *Jefatura de Polícia de Montevidéu*, não foram localizadas informações precisas sobre essa aquisição milionária.

Somente ao conferir o portal oficial da Agência Reguladora de Compras Estatales (ARCE) é que localizou o processo de licitação referente ao sistema de reconhecimento facial adquirido pelo MI. Trata-se da "Licitación Pública 13/2019"[4]: em seu chamado público, o Ministério demonstra interesse em adquirir uma licença para uso de uma plataforma de identificação facial, junto de seu respectivo serviço de suporte técnico, por três anos.

Instruído junto ao edital, o documento conta com anexos, dentre eles o ANEXO I que diz respeito aos requisitos excludentes e os de pontuação no processo licitatório. Destacam-se, dentre os requisitos: a exigência no item 28 de que o MI seja proprietário dos dados e das informações que dizem respeito ao funcionamento da plataforma; a obrigatoriedade de registro de todas as movimentações realizadas na plataforma que dizem respeito ao processamento e tratamento dos dados; o índice de desempenho de 95% para verdadeiros positivos e inferior a 0,01% de falsos positivos; processamento de imagens em definição de 4K; obrigatoriedade do algoritmo reconhecer as faces ainda que em condições diversas de iluminação, ângulo e zoom. Por fim, o ANEXO I ainda exige a entrega do Plano de Projeto Preliminar e de Gestão de Riscos do Projeto, em que em cada relatório devem constar as atividades previstas e os resultados entregues em cada etapa da implementação do projeto.

[4] Informações sobre o andamento da licitação 13/2019 no link: https://www.comprasestatales.gub.uy/consultas/detalle/id/744940 .

Demais informações referentes aos critérios pontuados pelas empresas que disputaram a licitação não foram divulgadas no site. De modo que não há como inferir quais itens a empresa selecionada cumpriu, indo desde os requisitos básicos até os desejados: o site também não tornou públicos os documentos referentes ao relatório de gestão de riscos e de implementação do projeto, ao ponto de não ser possível identificar em qual fase de implementação o projeto se encontra, quais foram os seus resultados e a avaliação deles e, tampouco, os indicadores de eficiência e eficácia utilizados em seu monitoramento (Gonçalves Feliz; Duarte, 2024). Caso o cidadão queira ter acesso a mais informações, lhe é disponibilizado um formulário para consultas.

A informação básica deve ser buscada de forma ativa pelo cidadão que deseja se informar do básico. E, em caso de ausência de resposta aos formulários ou demora excessiva, há ainda uma outra alternativa para se ter acesso ao mínimo de informação, a via judiciária.

4.2. Judicialização da demanda

Em busca realizada junto ao repositório da Base de Jurisprudência Nacional Pública, foi localizada a Sentença Definitiva nº 15/2023 do Tribunal de Apelaciones Civil 1º Turno [5] [6]. A sentença diz respeito ao Processo nº 2-66124/2022, cuja lide se resume ao recurso interposto no Contencioso Administrativo: no processo, Patrícia Diaz moveu ação em face do *Ministerio del Interior* a fim de ter acesso às informações referentes ao uso que se tem dado e planejamentos futuros quanto ao sistema de reconhecimento facial obtido pelo Ministério.

Na Corte Administrativa, identificou-se que a própria existência da informação requerida não era tema incontroverso, pelo contrário, o MI teria indicado que não teria acesso a esse tipo de informação e não soube informar os usos presentes e futuros da ferramenta por ele comprada. Na decisão impugnada, foi indicado que, ainda que o requerido tivesse posse da informação solicitada, não seria devido divulgá-la, ante o seu caráter reservado.

[5] Link para a busca junto ao site Base de Jurisprudencia Nacional Publica: https://bjn.poderjudicial.gub.uy/BJNPUBLICA/busquedaSimple.seam .

[6] TRIBUNAL DE APELACIONES CIVIL. Sentencia Definitiva **Nº 15/2023**. 1º Turma Civil. Redatora Min. Dra Beatriz Venturini. Publicação em 08/02/2023.

4.2.1. Uma aquisição milionária sem finalidade determinada

Na Corte de Apelação, a Relatora Min. Dra. Beatriz Venturini confirmou a sentença apelada. Em votação unânime, a Corte entendeu que sua decisão estaria restrita a determinar se a informação solicitada por Diaz existe ou não. Entretanto, diante da importância da matéria discutida e tendo em vista que se trata do único caso referente ao uso do reconhecimento facial discutido em sede judiciária, a Ministra ponderou alguns temas antes de pronunciar a decisão.

Inicialmente, destacou o entendimento majoritário sobre a natureza e relevância da informação pública. E, para sumarizar a jurisprudência, optou por aproveitar os julgados colacionados na sentença apelada:

> "Como se afirma por la Sala en su actual integración en Sentencia Nro. 155/2021: "En la actualidad el derecho de todas las personas a una **información 'oportuna, veraz e imparcial' sin censuras ni ocultamientos viene adquiriendo particular relevancia y ha sido incorporado expresamente en textos constitucionales recientes** (Brewer, Allan. La libre expresión y el derecho a la información en la Constitución Venezolana de 1999, en Anuario de Derecho Constitucional Latinoamericano, 2002 p.267-276). (...) 'Por su parte, tiene dicho la Suprema Corte de Justicia que tanto el **derecho a la información** como la libertad de prensa son '**derechos tan trascendentes que pueden ser ubicados en un plano superior al de otros derechos civiles pues de ello depende la estructura de las relaciones entre el poder y la libertad'** (Sentencia Nº253 de 13/10/99). Como señala Muñoz Lorente –citado en ese fallo- su prevalencia deriva fundamentalmente del interés público, de la función que cumplen como contribuyentes a la formación de opinión pública libre, inherente a todo sistema democrático (Muñoz Lorente, José. Libertad de información y derecho al honor en el Código Penal de 1995. Valencia, 1999, p.150.(...) 'Como la definición legal de la "información pública' adolece de marcada vaguedad, puesto que no exige que se trate de información 'de interés público', ni la limita a la referente, obtenida o producida por organismos públicos, de modo de diferenciarla de la 'información privada' (DURAN MARTINEZ, A. Derecho a la protección de datos personales y al acceso a la información pública. Montevideo, 2009, Ed. A. Fernández p.102)**, lo cierto es que viene a incluir toda aquella información que, por cualquier circunstancia 'esté en posesión' de un organismo público (arts.2 y 4)**" (TRIBUNAL DE APELACIONES CIVIL. Sentencia Definitiva Nº 15/2023. 1º Turma Civil. Redatora Min. Dra Beatriz Venturini. Publicação em 08/02/2023, grifo nosso).

Desse modo, a Corte de Apelações confere visibilidade ao debate em torno da relevância da informação pública prestada de forma ágil, integral e transparente como um direito constitucional e com especial peso na ponderação de interesses e princípios. Esse valor especial conferido à informação pública dá-se em razão dela ser um insumo fundamental para efetivar a participação cidadã na democratização da gestão pública.

Quanto à qualidade da informação prestada, foram incluídos extratos jurisprudenciais que dizem respeito ao dever do órgão público de prestar as informações de forma transparente e garantir o efetivo acesso às informações públicas:

> "Y de la misma forma, en Sentencia de la Sala Nro. 168/2015 se afirma: **"El objeto de la ley es "promover la transparencia de la función administrativa de todo organismo público, sea o no estatal, y garantizar el derecho fundamental de las personas al acceso a la información pública**. Es decir que el cuerpo trata de la información que se produce en los organismos públicos. Por ello es pública" (CF. Flores Dapkevicius en "El acceso a la información pública en Uruguay - Leyes 18.281 y 18.331", en L.J.U., Cita Online: D732/2011, Tomo: L.J.U. Tomo 143) (...) Carlos Delpiazzo además del principio de transparencia, señala los siguientes principios rectores: **a) principio de publicidad del obrar administrativo, el cual deriva de la forma republicana de gobierno; b) principio de legalidad, c) principio de consecución del interés público, d) principio de respeto por los derechos de los ciudadanos en el marco del bien común**; "métodos que tratan de promover los principios de colaboración ciudadana, de participación y de promoción de una nueva y diferente forma de concebir el poder administrativo más próximo a los ciudadanos"; e) **el principio de participación, según el cual, existiendo accesibilidad real, corresponde que los habitantes sean informados y consultados en los asuntos que les conciernen** ("A la búsqueda del equilibrio entre privacidad y acceso". Protección de datos personales y Acceso a la Información Pública, Instituto de Derecho Informático, Facultad de Derecho de la Universidad de la República, F.C.U. /AGESIC, Montevideo año 2009, pág. 9 y sig.)" (TRIBUNAL DE APELACIONES CIVIL. Sentencia Definitiva Nº 15/2023. 1º Turma Civil. Redatora Min. Dra Beatriz Venturini. Publicação em 08/02/2023, grifo nosso).

E, antes de pronunciar-se sobre o caso em concreto, a Relatora destacou os argumentos apresentados pelas partes: a autora sustenta que as atitudes do *Ministerio del Interior* indicam que a parte demandada tem o dever de prestar contas quanto ao fim que dará para a ferramenta adquirida, principalmente quando se leva em conta que o Ministério realizou um processo licitatório e gastou mais de um milhão de dólares na contratação do *software*; ao passo que o MI somente indica que não possui a informação solicitada.

Quanto ao argumento da apelante, a Corte entendeu que se trata de um raciocínio tendencioso formulado pela parte, de modo que as suas alegações indutivas carecem de lastro probatório. A mera presença de reuniões para discutir a elaboração e contratação do projeto não seria suficiente para determinar a existência da informação referente ao uso específico que se dará para a plataforma de reconhecimento facial.

Em outros termos, a autora não provou que a informação existia. Para além da discussão do ônus da prova desproporcional incumbido à cidadã, merece igual destaque outra justificativa utilizada pelo tribunal para respaldar a sua decisão, que consiste no fato de que, ainda que a apelante tivesse provado que a informação solicitada não existe, não seria dever do MI produzir as respostas solicitadas. Como respaldo jurisprudencial, foram colacionados breves argumentos da sentença apelada, Sentença nº 155/202:

> *"Se estima que es de aplicación al caso lo dispuesto por el art. 14 de la ley 18.333 que establece: 'La solicitud de acceso a la información no implica la obligación de los sujetos a crear o producir información que no dispongan o no tengan obligación de contar al momento de efectuarse el pedido'.En definitiva, el accionante afirma que el pedido por escrito tuvo lugar, y la parte demandada lo niega.**En tal disyuntiva no puede prohijarse un principio "en la duda en favor del accionante", pues ello sería violatorio del principio de igualdad y de las garantías del debido proceso**, reglas estas últimas no desvirtuadas por no haberse realizado una declaración de parte demandada que no es razonable pensar hubiera culminado en una confesión de existencia del documento que según se alega a lo largo del proceso no existe"*. A mayor abundamiento, volviendo al caso a estudio, no corresponde al Poder Judicial analizar la pretensa desidia de la comisión designada en elaborar el protocolo. El punto transcendente es que no está probado que la información exista, por lo que mal puede obligarse al Ministerio del Interior a brindar una información inexistente.(TRIBUNAL DE APELACIONES CIVIL. Sentencia Definitiva Nº 15/2023. 1º Turma Civil. Redatora Min. Dra Beatriz Venturini. Publicação em 08/02/2023, grifo nosso).

Por fim, ao decidir a causa sem julgar o mérito, a Relatora ainda destacou que não é cabível a discussão quanto à natureza da informação solicitada ser ou não de caráter reservado, tendo em vista que na defesa ministerial o órgão limitou-se a negar a informação solicitada unicamente com o fundamento de sua inexistência. Ao restringir a sua justificativa, as informações referentes ao objeto demandado estariam restritas à confirmação de sua existência.

Não há registros no banco nacional de jurisprudência de que o assunto tenha voltado a ser discutido ou que a decisão do Tribunal de Apelações, Sentença Definitiva nº 15/2023, tenha sido impugnada em fase recursal.

Nesse sentido, as conclusões que se pode tirar do recente pronunciamento judicial do único caso que trata do direito de acesso à informação referente ao uso das ferramentas de reconhecimento facial apontam para a falta de devida apreciação da temática. Não foi debatida a natureza da informação solicitada, se seria reservada ou pública, tampouco foi estabelecido um prazo para que a informação básica requerida seja produzida. Sequer foi decidida a necessidade de se prestar as informações quanto ao desenrolar do procedimento licitatório e à publicização dos relatórios de desempenho da tecnologia.

Entretanto, apesar de o argumento do MI ter sido sintetizado em uma frase, tal defesa lança luz a um fato preocupante: o órgão gastou um milhão de dólares dos cofres públicos para empreender em um projeto sem finalidade definida. Situação curiosa, quando se leva em conta que no edital da "Licitación Pública nº 13/2019" o ANEXO I é enfático ao determinar que todos os dados presentes na plataforma do *software* são propriedade do Ministério, bem como é imprescindível que todas as movimentações e processamentos realizados com os dados fiquem registrados.

Ademais, o anexo também destacava a necessidade de elaboração do relatório do projeto e de avaliação de cada uma de suas etapas, bem como o relatório de impacto e riscos. Resta a dúvida se todas essas informações também não existem.

Em caso afirmativo, o quadro apresentado se agrava. Pois, além de ter gastado uma parcela volumosa do orçamento previsto para a dotação anual, o MI, como proprietário dos dados e das informações relativas ao processo de implementação e funcionamento do sistema de reconhecimento facial, desconhece quais são as funções do próprio sistema que adquiriu e que finalidade se pretende dar a esse empreendimento. Tal cenário leva ao questionamento se, em algum momento, o Ministerio esteve em posse de qualquer informação básica ou se participou no processo decisório referente ao *modus operandi* da ferramenta.

Em outros termos, quando o *Ministerio del Interior* se coloca em posição de completo desconhecimento quanto ao uso e finalidade do sistema de reconhecimento facial, dúvidas são lançadas para o seu grau de envolvimento no projeto. Informações como histórico de movimentações dos dados e relatórios são postas em cheque. A própria existência dessas informações passa a ser questionável, ao ponto de se duvidar do fato do MI ser o proprietário dos dados. Os resultados do processo judiciário lançam desconfiança sobre o procedimento licitatório: o grau de cumprimento das exigências elencadas no ANEXO I, bem como a forma de funcionamento da tecnologia e seus índices de acerto, o seu banco de dados e as métricas dos algoritmos são postos em posição de desconfiança.

Por fim, ante a inexistência de informações básicas, cogita-se que, em momento algum, o Ministério tenha tido acesso às informações fundamentais para a implementação e uso do sistema de reconhecimento facial adquirido.

5. AS CÂMERAS NA PRAIA

No contexto brasileiro, o uso das câmeras de reconhecimento facial na segurança pública é intermediado por várias estratégias e centros de interesses. Desse modo, a fim de melhor delimitar o tema abordado neste trabalho, voltou-se a atenção para o uso dos sistemas de segurança e monitoramento no Estado do Ceará. Aqui, observa-se uma interessante intersecção das demandas do setor hoteleiro somadas ao clamor popular por segurança.

Antes marcado pelo olhar "seco" voltado para os seus terrenos áridos, ao final da década de 1990, o sertão cearense e suas belas praias ganharam um novo imaginário simbólico: o "pioneirismo" dos investimentos em um espaço privilegiado com alto potencial para a atividade turística (Dantas, 2009) e a viabilidade da fruticultura como uma solução para o desenvolvimento de uma agricultura repleta de vantagens comparativas (Elias D; Pequeno, 2013). Tais concepções são fruto do esforço, embora desarticulado, das políticas turísticas no Nordeste, como as orientadas pela CTI/NE (Comissão de Turismo Integrado do Nordeste), EMBRATUR (Agência Brasileira de Promoção ao Turismo) (Dantas, 2009) e do PRODETUR (Programa de Desenvolvimento do Turismo no Nordeste) (Elias D.; Pequeno, 2013). São programas e políticas públicas que buscam tornar a imagem do Nordeste mais atrativa para investimentos.

O resultado desses programas é indiscutível, uma modificação no "olhar" para os terrenos áridos e suas praias. Aqui, o "apelo" ao turismo tornou-se o catalisador do desenvolvimento regional, ao ponto de redefinir o consumo e a produção nesse espaço (Paiva, 2014). Todavia, os turistas não "aparecem" repentinamente. É necessário proporcionar uma infraestrutura para captar a sua atenção, dentre tantos destinos. E por infraestrutura se subentende a intersecção entre os variados mercados interdependentes do turismo: localidade, bom atendimento, hospitalidade, conforto, infraestrutura física, segurança, dentre outros (Silva Júnior, 2017). Destaca-se principalmente que o imaginário social invocado passa a ter impacto sobre a decisão de escolha quanto ao destino de viagem. Ao ponto que o noticiamento de matérias relacionadas com crimes violentos, como roubo e assassinatos, reforça o cenário de insegurança para o turista: esses dados, quando associados com a imagem social e econômica da região, impactam diretamente na demanda turística (Catai; Rejowski, 2004). Um dilema que perpassa o Nordeste.

5.1. O turismo estratégico

A construção e desenvolvimento do turismo no Ceará parte da conjunção de dois fatores principais, os de ordem econômica e o marketing desenvolvido em torno do litoral. Com o acesso ao Banco Interamericano de Desenvolvimento e aos repasses do Governo Federal nos projetos de desenvolvimento regional, o capital econômico ganha fôlego e destino quando se vê atrelado aos anseios da nova elite política: o volume expressivo de investimentos tem como destino o desenvolvimento turístico do litoral, como forma de proporcionar à região como um símbolo de sucesso e viabilidade do "novo" governo (Dantas, 2009). Encostas, praias e centros históricos, tudo isso, agregado ao imaginário cidadão de pertença a uma cidade turística, faz com que o Ceará, em especial a capital Fortaleza, seja percebido por seus moradores e investidores como uma região com "vocação turística" (Dantas, 2009). A propaganda mostra as praias e as vagas de emprego no setor hoteleiro.

Contudo, levou um tempo para chegar-se a essa colaboração entre o setor privado e o público. Inicialmente, o Ceará ocupava uma posição periférica na divisão do trabalho brasileiro: encaixava-se na pecuária extensiva, exportação de algodão e agricultura de subsistência, ao ponto de os lucros advindos dessas atividades representarem quase a totalidade do PIB do Estado (Elias; Pequeno, 2013). Esse cenário se modifica quando programas de estruturação econômica elencam como um dos eixos de desenvolvimento o turismo: em tais programas, se busca desenvolver metodologias e estudos de viabilidade das cadeias produtivas e das formas com que elas podem se difundir rapidamente, isso tudo, associado ao planejamento (Elias; Pequeno, 2013). O turismo passou a ser visto como uma potência.

As áreas litorâneas cearenses, com mais de 570 km de litoral, associados a 2,8 mil horas de exposição solar no ano e médias de temperaturas em 28 graus, são um privilégio turístico (Elias; Pequeno, 2013) que soube ser bem explorado.

Anunciado como uma forma de mitigar a pobreza, o desenvolvimento turístico tornou-se uma política pública. A potência do litoral carrega elementos que atuam como atrativos para o investimento na região, o que, consequentemente, gera circulação de renda, transferência de recursos e inovações tecnológicas (Silva Júnior, 2017). Principalmente quando se leva em conta as suas "possibilidades multiplicadoras", em áreas como alimentação, hospedagem, artesanato, bancos, transporte e comunicação, o turismo gera "uma nova dinâmica ao espaço, promovendo a expansão de fixos (infraestruturas de acesso, apoio, suporte) e, consequentemente, o aumento de fluxos de diferentes naturezas e intensidades" (Elias; Pequeno, 2013, p. 106). E seus impactos refletem na economia local.

A título de exemplo, em 2012 o turismo já representava mais de 10,8% do PIB do Ceará, enquanto como impacto indireto pode-se mencionar que mais de 50% das pessoas economicamente ativa estavam empregadas no setor de comércio e serviços (Paiva, 2014), áreas tipicamente impactadas pelo avanço turístico.

Diante de seu expressivo impacto econômico, ainda mais nos cofres públicos, o Governo do Ceará passou a tomar o protagonismo no desenho da imagem turística da região. Como "agente produtor do espaço", o Estado tornou-se o responsável pela criação da infraestrutura fundamental para o desenvolvimento e fruição da atividade turística: como estruturas de saneamento, aeroportos e rede rodoviária, marcos regulatórios de ocupação do solo e incentivos fiscais (Paiva, 2014). Há casos da participação de envolvimento do setor público na propaganda turística. Como no Governo Ciro Gomes, em que foi exigido que na filmagem da telenovela "Tropicaliente", exibida em 1994, pela Rede Globo, somente as partes com infraestrutura turística e "modernas" deveriam ser filmadas (Paiva, 2014).

Nesse cenário de constante movimentação, seja de ativos financeiros ou de pessoas, o Ceará se transforma em uma região altamente globalizada. Um espaço que se conecta ao mundo, ao interagir constantemente com ele, ao ponto de passar por uma incessante mutabilidade:

> "(...)Como objeto e sujeito da economia globalizada, é um espaço que pouco tem de autônomo, não se encerrando sobre si mesmo, de forma independente do resto do mundo, com o qual interage permanentemente no processo de acumulação de capital. Nos últimos vinte e cinco anos, é visível sua reestruturação econômica e, consequentemente territorial, com objetivos claros de inserir-se na lógica da produção e do consumo globalizados" (ELIAS, D.; PEQUENO, 2013, p.99).

A região não se vê livre de influências externas, pelo contrário, é por elas estruturada. Ao ponto de ser uma região tocada pela expansão do capital e palco das novas tecnologias. Todavia, o manto do "desenvolvimento" econômico não cobre toda a extensão do território cearense, pelo contrário, são poucos os locais que usufruem dessa especial atenção.

Os lucros da globalização não são distribuídos de forma equânime, o crescimento econômico não veio acompanhado do desenvolvimento da região. Os projetos estruturantes nos municípios são precarizados e o mercado imobiliário é altamente especulado: a inserção do Ceará no Mercado deu-se de forma "conservadora" com vistas a manter as estruturas sociais já existentes, de modo que os "privilégios da modernização" sejam restritos a territórios seletos (Elias; Pequeno, 2013).

Entretanto, o desenvolvimento fragmentado das regiões não litorâneas torna essas áreas mais vulneráveis à violência e, com a ausência de investimento em políticas de combate à criminalidade atreladas ao conjunto de ações socioeconômicas, essa vulnerabilidade é acentuada (Silva Júnior, 2017).

O Ceará ocupou, em 2012, o terceiro lugar dentre os maiores índices de homicídios por cem mil habitantes: seus números eram de 44,6, atrás apenas do Espírito Santo com 47,3 e Alagoas com 64,6; observa-se que nessa época a média do Sudeste foi de 21 (Silva Júnior, 2017). A imagem das praias paradisíacas contrasta com os homicídios noticiados pela mídia nacional. Com taxa anual de 38,9 homicídios por 100 mil habitantes, o Nordeste alcançou o patamar de "violência epidêmica" na classificação da Organização Mundial da Saúde (OMS) (Silva Júnior, 2017). Um cenário alarmante e surpreendente, quando se leva em consideração que a demanda turística de Fortaleza teve um acréscimo de 62,1% entre 2006 e 2015, com média de crescimento anual por volta de 5,5% (Silva Júnior, 2017).

O aumento no fluxo de turistas não seria esperado. Principalmente quando se leva em conta que, ao escolher a rota de viagem, os turistas visam o descanso e buscam evitar eventos de violência, ao ponto de mudarem de destino se a estadia não for segura e protegida (Silva Júnior, 2017). Com consumidores tão sensíveis, o comércio torna-se sensível.

Em sua dissertação de mestrado, Silva Júnior (2017) apresenta o impacto econômico nos cofres públicos, proporcionado pelo aumento nos índices de criminalidade que pode proporcionar e o consequente decréscimo na arrecadação com o turismo. Seu estudo leva em conta a relação entre a taxa de criminalidade, refletida no índice de homicídios por 100 mil habitantes, e a demanda turística, refletida nos índices de ocupação em hospedagens. Os resultados surpreendem, para cada aumento na unidade da taxa de criminalidade, o Ceará perdeu R$ 8,18 milhões em arrecadação, ao passo que no ano a perda em arrecadação turística direta alcança a soma de R$ 369,49 milhões (Silva Júnior, 2017).

Ante o expressivo prejuízo econômico, fez-se necessária a adoção de estratégias de combate ao crime e melhoramento da imagem regional. Aqui, a estratégia varia entre a modernização das tecnologias utilizadas na vigilância dos espaços públicos e o investimento no policiamento comunitário. A despeito da eficácia questionável dessas medidas, um dado é incontroverso: a demanda turística reagiu bem a esses incentivos.

A propaganda mostra-se eficiente. Como uma forma de angariar investimentos para a região, faz-se necessária a construção e manutenção da "imagem turística", tendo em vista que, como uma política de Estado, é necessária a colaboração e consenso de que o turismo faz parte do interesse público (Paiva, 2014).

É uma construção do espaço rico em infraestrutura e suporte para o turista, um espaço seguro. As formas de se pensar estrategicamente a construção desse espaço imaginário contam com o investimento no "*marketing*" e promoção da boa imagem dos órgãos de policiamento.

5.1.1. A imagem da ronda e seus herdeiros

Nas eleições de 2006, o então candidato a governador Cid Gomes, irmão de seu antecessor, optou por continuar a campanha de desenvolvimento da "imagem" do Ceará. Antes voltada para angariar investimentos no ramo turístico, as novas gestões passaram a se preocupar com as notícias da crise na segurança pública e na forma como elas poderiam afetar o Estado. Nesse sentido, o candidato, em sua campanha de 2006, voltou seus esforços para o combate à onda de violência, em um movimento caracterizado por politizar os problemas da segurança pública: medo, violência e insegurança percebida pelos cidadãos foram utilizados como estratégia eleitoral (Araújo, 2019). Empossado, Cid Gomes decide pôr em prática as suas promessas de campanha, buscando, então, as "modernas" estratégias estrangeiras.

Em meados de 2007 e com extensão até o final de seu segundo mandato, em 2015, foi implementado na região metropolitana de Fortaleza o "Programa Ronda do Quarteirão": composto por policiais novatos, o programa foi montado com o intuito de "limpar" a imagem da "velha polícia" militar (Ribeiro, 2024). Com fardas desenhadas por um estilista renomado e equipados com uma frota de dez carros modelo Hilux, o novo batalhão contou com os aparatos tecnológicos de ponta e uma estrutura "moderna" para proporcionar um patrulhamento de qualidade nos bairros: a meta inicial era aproximar a comunidade do corpo policial, buscando eliminar as conotações negativas pré-existentes e proporcionar maior engajamento do cidadão com os temas da segurança pública (Araújo, 2019).

O maior batalhão de segurança na América Latina, o "ronda" contava com cadetes graduados com um curso de formação, cujas disciplinas variaram entre comunicação, mediação de conflitos, proteção dos direitos e garantias individuais e aulas de etiqueta: a preocupação com a estética e produção midiática do batalhão proporcionou maior destaque às ferramentas modernas agregadas ao corpo policial; em que o efeito político conferiu visibilidade à aquisição de viaturas, uniforme e tecnologias de vigilância, elementos que, até então, passavam despercebidos pela opinião pública (Araújo, 2019). A título de exemplo, a frota de carros contava com câmeras internas e computador de bordo: no monitor era possível pesquisar a ficha criminal dos acusados e obter informações sobre as placas dos veículos (Araújo, 2019). Ocorre que as viaturas eram modernas demais.

Essa polícia adaptada à comunidade não tardou a ser recepcionada com descrença e desconfiança. Antes com 72% de índice de aprovação, número imprescindível para garantir a legitimação do projeto, a imagem do novo batalhão foi "maculada" com os elevados números de incidentes na condução das modernas viaturas: o corpo policial não estava pronto para o seu uso e os incidentes, aliados à burocracia para consertar os veículos, tornaram uma parcela considerável da frota indisponível para o uso (Araújo, 2019). O investimento nesses carros de elevado valor agregado passou a ser questionável.

A política adotada para evitar maiores incidentes foi a de reduzir a velocidade dos veículos remanescentes para 50km/h, situação que não tardou a ser motivo de chacota (Araújo, 2019). Casos de corrupção e flagrantes de condutas ilegais dos membros do batalhão, filmados pelas próprias câmeras das Hilux, minaram ainda mais a opinião popular (Ribeiro, 2024). Com o corpo policial incomodado com a crescente descredibilidade da "ronda", os membros do batalhão passaram a agir com maior truculência nas abordagens policiais, com vistas a "legitimar" a existência do novo batalhão (Araújo, 2019).

Com o fim do mandato de Cid Gomes, o "Programa Ronda do Quarteirão" foi desarticulado e minguou. Entretanto, os esforços midiáticos de promoção da imagem da segurança pública não foram desmobilizados, pelo contrário, ganharam "novas roupagens" com o tecnosolucionismo das ferramentas de vigilância.

Na gestão de Camilo Santana, 2015-2022, o Governador viu na modernização dos serviços de videomonitoramento e expansão do policiamento ostensivo a solução para a crise nos índices de criminalidade: através do direcionamento de recursos para setores destinados ao desenvolvimento de soluções tecnológicas, a segurança pública iria se mostrar mais eficiente (Ribeiro, 2024). Em outras palavras, a prometida "modernização" era uma velha conhecida:

> "Não há uma ruptura entre uma política e outra. **Há, na verdade, uma incorporação sob o prisma da integração das ações governamentais, com filiação às demandas do contexto local, nacional e internacional. Todas as tendências convergem para uma prática de manutenção no campo da segurança pública.** Por ser um campo intelectual, mas também político, as práticas adotadas nesse contexto acabam reproduzindo um modo de fazer específico que intervém para a manutenção do próprio campo. **No Ceará, as políticas adotadas nos últimos 25 anos no campo da segurança pública são constantemente carregadas de elementos da política anterior, porém sob aparência do "novo"**. [...] esse "novo" se coloca de diferentes formas, seja pela mudança das viaturas ou da farda, criação de um outro slogan, etc." (LINS, 2020, p.78 in Ribeiro,2024, p.101, grifos nossos).

Na reiteração da velha política que já vinha sendo apresentada, a nova gestão optou por investir no movimento tecnológico.

Entretanto, com vistas a evitar que os novos operadores “desperdicem” os investimentos por falta de preparo técnico para conduzir as novas ferramentas, foi-se feito um investimento massivo na criação de departamentos específicos para a condução da “nova” empreitada tecnológica.

Nesse contexto, a recém-criada Superintendência de Pesquisa e Estratégia de Segurança Pública do Ceará não tardou a lograr esforços para “mostrar serviço”. Suas estratégias, aliadas às movimentações da Secretaria de Segurança Pública e Defesa Social do Ceará, direcionaram-se principalmente ao movimento político e propagandista das instituições: as falas de seus principais dirigentes evocam a eficiência e agilidade da tecnologia no número de prisões e índices de bens recuperados como forma de justificativa para o uso das próprias ferramentas tecnológicas (Ribeiro, 2024).

Os esforços de promoção da imagem da instituição não possuem informações pormenorizadas sobre o funcionamento das ferramentas adquiridas ou em fase de testes. Pelo contrário, consistem em “operações policiais videodirecionadas” que visam o engajamento do cidadão na “rotina” policial: o material publicizado consiste em vídeos com menos de um minuto, veiculados no YouTube e Instagram, que contam com “flagrantes” policiais proporcionados com o auxílio das novas ferramentas de vigilância (Ribeiro, 2024).

Entretanto, há um contraste entre a informação publicizada e as que deveriam ser públicas. É necessário um esforço desproporcional por parte do cidadão para ter acesso às informações básicas relacionadas às ferramentas que são utilizadas na segurança pública cearense. A título de exemplo, enquanto os anúncios nas mídias digitais informam os resultados das “novas” aquisições tecnológicas, descobriu-se, por meio de requerimento dirigido ao portal Ceará Transparente, que desde 2000 o reconhecimento facial já é utilizado na forma de aplicativo para os celulares utilizados pelo corpo policial:

> “(...) desde 2020 no estado do Ceará já se efetuam prisões fazendo uso de reconhecimento facial por meio do uso policial do aplicativo PCA. Atualmente, conforme apontam os dados oficiais, obtidos por meio de lei de acesso à informação (LAI) junto ao portal eletrônico Ceará Transparente, pela pesquisa de Martins et al. (2024, p.11), o PCA seria a única tecnologia operada pelas forças estaduais de segurança a ter a funcionalidade do reconhecimento facial (TRF): **A função de reconhecimento facial realiza o cruzamento de fotos tiradas pelos agentes ou baixadas no celular com uma base contendo mais de 8 milhões de perfis cadastrados no Estado. O algoritmo faz a comparação na base de dados e retorna com os dados da pessoa identificada**. É um importante instrumento de apoio para a ação das forças policiais, contribuindo tanto para a prevenção de delitos quanto para a solução de crimes. O Ceará é um dos pioneiros do Brasil a utilizar a pesquisa por reconhecimento facial a partir de um aplicativo de celular, o PCA, que pode ser baixado diretamente no dispositivo do profissional da segurança pública do Ceará” (Ceará Transparente, 2021 apud Martins et al., 2024) (RIBEIRO, 2024, p.205).

Nesse cenário de escassez de informações, cabe à Superintendência de Pesquisa e Estratégia de Segurança Pública do Ceará e à Secretaria de Segurança Pública e Defesa Social do Ceará divulgar os boletins informativos quanto aos serviços contratados, à forma como eles operam, ao banco de imagens utilizado e aos algoritmos envolvidos no sistema. Não há vislumbre de qualquer relatório do tipo, pelo contrário, as informações divulgadas se limitam a repetir a propaganda da tecnologia adquirida e justificar o seu uso com as estatísticas. Nessa "custódia informacional" faz parte do movimento de modernização, em que o "monopólio" da informação, inclusive das próprias métricas utilizadas nas estatísticas, dá lugar às divulgações periódicas que evocam a "positividade tecnosolucionista" (Ribeiro, 2024).

A informação divulgada passa a ser a única disponível e, consequentemente, se torna um dado absoluto. Quando a tecnologia é descrita somente com base em seus resultados e na sua "necessidade", esses dados passam a ser suficientes para resumi-la.

Contudo, os resultados "positivos" e a "redução" da criminalidade são postas em xeque quando confrontados com o salto nos índices de Crimes Violentos Letais Intencionais (CVLI). Nas estatísticas divulgadas pela Secretaria de Segurança Pública e Defesa Social do Ceará (2024), os números de mortes provocadas por homicídios, latrocínios e lesão corporal seguida de morte alcançaram os 3.272 óbitos, somados às 189 vítimas decorrentes da intervenção policial. Em 2022 e 2023, foram registrados os mesmos números decorrentes de CVLI, 2.970 óbitos; enquanto no ano de 2023 houve um acréscimo de 12,9% do índice em relação a 2022, 878 e 778 mortes respectivamente (SSDPS, 2023). Observa-se que, apesar do fim do mandato de Camilo, a estratégia utilizada para "combater" o crime continua a mesma.

Em sua fala, o então governador do Ceará, Elmano Freitas, anunciou, em 26 de agosto de 2024, que não iria poupar esforços para modernizar a polícia cearense no combate ao crime:

> "Não vamos recuar no enfrentamento implacável ao crime, para dar garantia de tranquilidade e paz ao cidadão. Por isso, anunciamos concursos para as Forças de Segurança, além de chamar mais aprovados no concurso da Pefoce. Para ter mais força e ação, com as tecnologias vamos desestimular a ação criminosa em todo território cearense" (FREITAS, 2024 in Ceará Gov,2024).

A estratégia do "ronda" parece ter ganhado novos contornos. Policiais recém-formados e munidos com a tecnologia de ponta serão a "nova" aposta para a segurança pública do Ceará. Nesse retorno das políticas de vigilância, um detalhe costuma passar despercebido: a própria aquisição das tecnologias utilizadas no policiamento e "manutenção da paz" não é discutida e tampouco anunciada. Nesse sentido, o próximo tópico irá se debruçar sobre as formas de aquisição das ferramentas de videomonitoramento e seu amparo jurídico.

5.2. As políticas de aquisição da tecnologia

Em consulta ao portal Sistema de Gestão Governamental por Resultado do Governo do Estado do Ceará, na seção que diz respeito ao bloco Licita Web, foram identificadas as contratações referentes à aquisição de sistemas de videomonitoramento. Ao todo, foram 54 registros em todo o Estado, desde 2013 até 2025. Destes registros, merecem destaque as aquisições da Superintendência da Polícia Civil do Estado do Ceará.

Inicialmente, o que chama a atenção é a quase totalidade de contratações entre a Polícia Civil e a Empresa de Tecnologia da Informação do Ceará (ETICE). A título de ilustração, no Edital nº 20230021[7] a ETICE foi a vencedora do processo licitatório: o objeto de contratação era aquisição de serviço de videomonitoramento para manutenção das atividades da instituição e o valor total contratado é de R$ 50.439.955,68. O edital contou com dispensa de licitação, a justificativa deu-se com base no fato da contratação ser celebrada com entidade que integra a Administração Pública.

Na seção do Licita Web dedicada a divulgar as informações referentes ao processo licitatório, só foi localizado o arquivo "LISTA DE ITENS – ESPECIFICAÇÕES E QUANTITATIVOS". Nele, os itens informados são descritos por meio de dois agrupamentos: "1597950 - Serviços de Provimento, Gerenciamento, Sustentação, Administração de Solução de Ponto de Monitoramento"; "1597960 - Serviços de Provimento, Gerenciamento, Sustentação, Administração de Solução de Captura 1 com Gerenciamento e Armazenamento em Nuvem". Não há informações adicionais no documento.

Nos demais processos licitatórios, o padrão tende a se repetir. As exceções representam as licitações suspensas ou revogadas, como no caso do Edital nº 20210117[8], licitação do tipo Menor Preço e com status revogado. O objeto licitatório foi descrito como "Aquisição de equipamentos de videomonitoramento, com instalação, para a Polícia Civil do Estado do Ceará".

---

[7] Informações sobre o edital 20230021 disponíveis no link: https://s2gpr.sefaz.ce.gov.br/licita-web/paginas/licita/Publicacao.seam?cid=38276 .

[8] Informações sobre o edital 20210117 disponíveis no link:https://s2gpr.sefaz.ce.gov.br/licita-web/paginas/licita/Publicacao.seam?cid=38522

A seção dedicada ao processo licitatório no site Licita Web conta com vários documentos anexados, dentre eles se destaca o Edital: no documento há as especificações dos equipamentos a serem comprados e as exigências para o seu funcionamento, tais como a inclusão de *software* de gerenciamento de imagens, geração de metadados com informações das pessoas e veículos identificados, pesquisa por face semelhante e ao vivo, câmeras com leitura de placas e estatística de estacionamentos.

Observa-se, em uma análise preliminar desses dois exemplos, a discrepância de informações. Nas licitações milionárias envolvendo a ETICE, sequer é possível identificar os equipamentos e serviços prestados, enquanto nos processos que foram revogados ou suspensos o edital é enfático ao determinar os requisitos mínimos de funcionamento das ferramentas tecnológicas para que os interessados logrem participação no processo licitatório.

Entretanto, ao se aprofundar na análise das aquisições de soluções de videomonitoramento, um dado chama a atenção: a empresa ETICE não produz a tecnologia. Em consulta ao Manual de Serviços da Etice, disponibilizado em sua página na web, é possível constatar que a empresa atua como uma intermediadora de serviços. Destacando-se por suas soluções tecnológicas, a empresa conta com os serviços de outras empresas de tecnologia, como a Google, IBM e Huawei, e intermedia a contratação dos serviços dessas empresas parceiras. Em outras palavras, quem presta o serviço final para a Polícia Civil do Estado do Ceará pode ser qualquer uma dessas empresas parceiras.

Essas contratações de tecnologias voltadas para a segurança pública e policiamento, em que pouco se sabe do objeto e serviço adquirido e muito menos de quem presta o serviço final, ganharam força com o amparo legal proporcionado pela Portaria Ministerial nº 793/2019 do Ministério da Justiça e Segurança Pública.

5.2.1. A Portaria do Ministério de Segurança Pública

Em 2019, foi editada pelo Gabinete do então Ministro da Justiça e Segurança Pública, Sérgio Moro, a Portaria nº 793 que regulamenta os incentivos financeiros ao combate ao crime e as condições para receber os recursos (Brasil, 2019). Essa portaria indica que os recursos serão transferidos diretamente do próprio Ministério para os fundos de segurança pública de cada estado. Dentre as ações financiáveis, destacam-se as do Eixo de Combate ao Enfrentamento à Criminalidade Violenta:

> "Art. 4º O Eixo Enfrentamento à Criminalidade Violenta compreende o conjunto de medidas para redução e controle da violência e da criminalidade, a serem desenvolvidas em territórios que apresentam altos indicadores criminais, ampliando a percepção de segurança e proteção social, por meio de ações multidisciplinares, intersetoriais e de integração de atores nas diversas esferas. § 1º O Eixo a que se refere o caput será composto pelas seguintes ações: I - realização de diagnósticos e planos locais de segurança; II - realização de ações de prevenção à criminalidade violenta;**III - reaparelhamento e modernização das instituições de segurança pública, com vistas à prevenção ou à repressão qualificada e à redução da criminalidade violenta e de enfrentamento ao crime** organizado, com destaque para as seguintes linhas de atuação: a) fomento à implantação de sistemas de comunicação operacional, como radiocomunicação, telefonia móvel e internet;b) f**omento à implantação de sistemas de videomonitoramento com soluções de reconhecimento facial, por Optical Character Recognition - OCR, uso de inteligência articial ou outros;** c) fomento à implantação de solução tecnológica para inteligência, atendimento e registro único de ocorrências, centrais de despacho, georreferenciamento de viaturas, **policiamento preditivo**, e câmeras corporais ou veiculares; d) construção, reforma, ampliação, **adequação e estruturação tecnológica de espaços e edicações para a gestão e governança integradas de ações de segurança pública**;" (BRASIL, 2019, grifos nossos).

Dentre os objetivos do Eixo de Enfrentamento à Criminalidade Violenta, são mencionados os incentivos a medidas de modernização dos equipamentos e o desenvolvimento de mecanismos de monitoramento dos projetos e avaliação de suas ações. Quanto aos resultados esperados, é indicado que se espera a impessoalidade nas investigações, aumento do índice de resolução dos crimes, redução do número de mandados de prisão em aberto. No que diz respeito aos impactos esperados, projeta-se a redução dos índices de criminalidade, impunidade e melhoria da credibilidade das instituições de Segurança Pública aliada ao aumento da percepção subjetiva de segurança (Brasil, 2019).

A notícia desses repasses orçamentários para a segurança pública estadual foi bem recepcionada pelos entusiastas da modernização. Esses recursos financeiros representam o passaporte para a aquisição das novas tecnologias de vigilância. Pois, até então, não havia qualquer marco jurídico vigente que regulasse o uso de tecnologias de monitoramento.

Em 2019, a única regulação dessas tecnologias dizia respeito às formas de se ter acesso aos repasses do Ministério da Justiça e Segurança Pública. Detalhamentos sobre as tecnologias vedadas, os seus limites, assim como quais são os direitos dos cidadãos vigiados e deveres dos centros de operação de repressão ao crime, tudo isso ainda deveria esperar por legislação própria. Contudo, em 2020, com a vigência da Lei Geral de Proteção de Dados Pessoais, esse cenário sofre modificações.

5.2.2. A LGPD e a Cobertura da Segurança Pública

A Lei Geral de Proteção de Dados Pessoais, de forma direta e objetiva, elenca já em seu primeiro artigo o seu objetivo principal: proteger os direitos fundamentais da liberdade e privacidade dos cidadãos, com vistas a lhes garantir o pleno e livre desenvolvimento de sua personalidade (Brasil, 2018). Seus fundamentos estão indicados no art. 2º e destacam-se o respeito à privacidade e a autodeterminação informativa. Quanto às definições previstas na lei, o art. 5º faz a sua devida cobertura:

> "Art. 5º Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável; **II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;** III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento; **IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico**; V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento; VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; (...) **X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração**; XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo; **XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinad**a (...)" (BRASIL, 2018, grifos nossos).

Inicialmente, destaca-se a definição conferida aos dados, um conceito expansionista que agrega toda e qualquer informação capaz de identificar o titular, ou que, ao menos, guarde a potencialidade de identificá-lo (Silva, 2023). Nesse contexto, os dados ganham especial proteção legislativa, pois são informações que expressam a individualidade do cidadão e da pessoa jurídica. Os dados pessoais são características intrínsecas aos titulares ao ponto de serem a extensão de sua personalidade: são representações do indivíduo na sociedade e formas pelas quais ele possa ser identificado (Silva, 2023).

Os dados atuam como os "vetores" da personalidade, pois traduzem para caracteres escritos ou numéricos, até mesmo estatísticas, as individualidades dos titulares.

Nesse sentido, ao atuarem como “projeções” da personalidade, qualquer lesão aos dados ou tratamento sem o consentimento do titular acaba por ferir a própria personalidade do indivíduo e, consequentemente, lesar a sua dignidade (Silva, 2023).

Em 2022, por meio da Emenda nº 115 de 2022, a proteção aos dados pessoais passou a figurar de modo expresso na Constituição Federal, como um direito fundamental, na forma do art. 5º LXXIX (Brasil, 2022). Importante destacar o teor econômico das discussões que ponderavam a necessidade de especial proteção para os dados pessoais. No bojo dos argumentos utilizados tanto para aprovar a LGPD quanto para consagrar a proteção dos dados pessoais na Constituição, o interesse dos investidores e a segurança jurídica dos contratos foram ponderados e tiveram peso decisivo: a presença de um marco regulatório pormenorizado confere segurança aos negócios, principalmente quando são contemplados os valores como transparência e monitoramento no fluxo de dados (Souza; Acha, 2022).

Ademais, antes da emenda, a proteção de dados pessoais já se encontrava compreendida nos desdobramentos do direito à intimidade e privacidade. A Constituição tutela, em seu sentido amplo, a proteção dos direitos à privacidade, de modo que honra e imagem também são amparados: na análise conjunta desses direitos, é conferida a proteção ao particular, seja em suas interações pessoais e expressões faciais; a privacidade confere também o direito de não ser vigiado, registrado e reconhecido (Silva, 2023).

Contudo, a LGPD, em seu art. 4º foi enfática ao determinar que os dispositivos por ela abrangidos não se aplicam ao tratamento de dados pessoais realizados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão penais (Brasil, 2018). A regulação dos mecanismos de tratamento e seus limites no âmbito da segurança pública ficou a encargo de lei posterior, que ainda não foi editada.

Entretanto, com vistas a evitar o completo desamparo desses dados e visando coibir abusos e violações de direitos, o art. 4º ainda determina que:

> “§ 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei” (BRASIL, 2018).

Nesse sentido, destaca-se a natureza principiológica da LGPD que, ao fazer prevalecer princípios em detrimento das regras, conduz os operadores do direito na linha das velozes mudanças tecnológicas, ao passo que favorecem o "dinamismo" da proteção dos dados pessoais: seus princípios modelam a aplicação da lei ao ponto de que devem ser aplicados em qualquer tratamento de dados, com vistas a evitar violações de direitos (Silva, 2023).

Quanto a esse dinamismo do mundo dos fatos e das novas tecnologias, o "princípio da precaução" se destaca como mecanismo apto a assimilar a letra do direito ao contexto prático. Tal princípio parte da necessidade de refazer o "desenho" das relações regulatórias, com vistas a minimizar as assimetrias de poder:

> "Nesse sentido, o princípio da precaução reconheceria as assimetrias de poder e de informação dos processos de avaliação regulatória e aj**udaria a remodelar os diferentes conhecimentos dos diversos atores envolvidos e afetados por esses processos (Stirling, 2016, p. 649). Trata-se, assim, de assumir compromissos com a deliberação e a accountability, assegurando justificações explícitas e cuidadosas sobre as escolhas regulatórias feitas diante de um "conhecimento incompleto"** - algo que, inclusive, fomentaria e criaria obrigações para com a pesquisa e o conhecimento científico, com vistas a obtenção de informações sobre os riscos desconhecidos" (HARTMANN, 2012; BIONI; LUCIANO, 2019, p. 213).

Quando aplicado nas relações entre titular dos dados e operadores, o princípio da precaução atua para dirimir as discrepâncias de informação que o polo mais fragilizado, o titular, possui em relação a quem trata os seus dados. Nesse sentido, o princípio busca mitigar as incertezas que o titular possui, principalmente quanto ao uso e manipulação de seus dados pessoais. Por meio de sua "arquitetura precaucionária de danos", desenvolve mecanismos que visam diminuir as possibilidades de violações de direitos (Bioni; Luciano, 2019).

Por fim, o princípio da precaução ganha força frente ao cenário de constantes mudanças tecnológicas em que os dados pessoais estão inseridos. Antes limitados à coleta por meio de entrevistas, os dados pessoais passaram a ser coletados por meio de redes sociais e até mesmo nas ruas públicas e centros comerciais.

Cada transeunte é tido como um potencial consumidor, ao ponto de que qualquer "rastro" ou "resto" de informação deixada possui valor agregado. Desse modo, ao estabelecer a necessidade de impor limites e reforçar a exigência de ferramentas que reduzem os impactos negativos da exploração dos dados, o princípio da precaução, quando aliado com a proteção constitucional à privacidade, é um mecanismo necessário para o estudo e implementação das tecnologias de videomonitoramento na segurança pública.

6. CONCLUSÃO

As câmeras, esse objeto discreto, sutil e “amigável”, são tidas como a nova aposta para o combate da criminalidade, seja no Brasil ou no Uruguai. Os incentivos fiscais, a constante exposição midiática, atrelados à falta de limites impostos pelo ordenamento jurídico, favorecem a propagação desses objetos.

No Ceará, a “nova” política das tecnologias já conta com décadas de existência. Seus registros mais distantes remontam ao uso das câmeras para vender a imagem das praias paradisíacas do litoral cearense. Esse objeto “sutil” atua desde então na guerra de narrativas: de um lado, o noticiário com as constantes taxas de aumento dos crimes violentos intencionais, enquanto na outra ponta, as câmeras proporcionam a propaganda do desenvolvimento cearense. Contudo, ante o volumoso investimento do capital estrangeiro no litoral, a região precisava ser mais atrativa para os viajantes e, para isso, contou com a propaganda dos próprios moradores. Além da sensação coletiva de pertencer a uma cidade com “vocação turística” (Dantas, 2009), os cidadãos passaram a tecer elogios para as inovações tecnológicas.

O turista, como um indivíduo altamente sensível às pressões da violência, busca no noticiário e nos moradores informações relativas à segurança do destino turístico (Silva Júnior, 2017). Nesse sentido, a aprovação popular das estratégias de monitoramento e combate ao crime passa a ser essencial na manutenção da demanda turística.

Entretanto, manter os elogios ao “ronda” é uma tarefa árdua. O incessante repasse de recursos financeiros e a destinação “inapropriada” deles podem ter um efeito negativo na aprovação da política pública. Desse modo, a “nova” estratégia política deve sempre ter em conta o “cálculo eleitoral” (Ribeiro, 2024) e nada mais convincente do que apostar na modernização do corpo policial. A estratégia se repete reiteradas vezes e a tendência é continuar com esse padrão, principalmente quando um dos principais problemas relativos à aprovação popular está resolvido.

A Portaria Ministerial nº 793/2019 incorporou os anseios dos governos estaduais e elaborou mecanismos de acesso ao fundo do Ministério da Justiça e Segurança Pública. Desse modo, os projetos que visam o combate à criminalidade e buscam reduzir os CVLI já podem contar com os repasses do Ministério. Em outros termos, a verba para a manutenção da imagem institucional não irá trazer prejuízos aos cofres do ente estatal.

Como artifícios que promovem a "espetacularização institucional", as modernas tecnologias de monitoramento são utilizadas para registrar e publicizar o "sucesso" do patrulhamento: seja nas perseguições ou cumprimento de mandados, as câmeras de videomonitoramento cumprem com o seu papel de gerar "lucros simbólicos e políticos" (Ribeiro, 2024). Entretanto, ao serem figurantes na propaganda institucional, os transeuntes ficam sujeitos aos riscos do monitoramento.

Desde o ano 2000, aplicativos de reconhecimento de imagens já estavam presentes nos celulares dos oficiais e eram usados para o cumprir mandados de prisão em aberto e realizar prisões em flagrante (Ribeiro, 2024). Ocorre que a tecnologia está em constante modificação, ao ponto de postar-se a todo tempo como "inovação".

A ferramenta utilizada pelo corpo policial cearense desde 2000 pode já estar ultrapassada e apresentar defeitos, assim como as atuais. Contudo, a desatualização da tecnologia não é o único fato preocupante, o desconhecimento de sua própria existência é igualmente alarmante. O transeunte pode fazer parte das estatísticas da propaganda tecnológica sem que sequer tenha ciência desse fato.

Contudo, nesse cenário de completo alheamento quanto ao uso das tecnologias de monitoramento, os Estados também representam os seus papéis. O primeiro deles diz respeito à intenção de manter a insegurança jurídica, no que tange ao tratamento dos dados pessoais para fins de segurança pública e repressão criminal. Outro personagem diz respeito ao comprador bem-intencionado que gasta milhões na esperança de ser moderno.

A narrativa da licitação uruguaia dialoga com os procedimentos licitatórios cearenses. No primeiro caso, o *Ministerio del Interior* buscou investir um milhão de dólares em um sistema de reconhecimento facial que sequer sabia as informações básicas de funcionamento. Após o gasto de verba pública, o sistema sequer pode entrar em funcionamento, pois o MI desconhecia a função que daria para a ferramenta que adquiriu.

Tal narrativa só não impressiona mais do que a primeira discussão normativa quanto ao tema do reconhecimento facial ter se dado em uma lei orçamentária. Nas discussões referentes ao Pressuposto Nacional, o Estado adotou o personagem que busca manter a insegurança jurídica. A preocupação quanto ao uso dessa postura pode ser traduzida pela fala da Senadora Nane: *"Nuevamente expresamos nuestra preocupación al respecto y lamento muchísimo que este debate no se haya instalado, por lo menos, con el compromiso por el futuro que entendemos, debió haber sido necesario"* (Nane, 2020 in Asunto 147701,2020).

Entretanto, a "brecha" da segurança pública não pode ser utilizada em investimentos desproporcionais e desnecessários:

> "Si bien el tratamiento de datos personales con fines de seguridad publica sin el previo consentimiento de sus titulares por parte de Organismos Policiales **está autorizado por el art. 25 de la LPDP, su inciso final establece que las bases de datos en tales casos "deberán ser específicas y establecidas al efecto".** Este inciso final adquiere especial relevancia con relación a datos sensibles como son los datos biométricos.En relación con esto, entendemos que difícilmente pueda interpretarse **la expresión "fines de seguridad pública" como un fin específico o claramente definido, particularmente por la indeterminación inherente al concepto seguridad pública"** (SANTOS DE AMORES, 2022, p.122, grifos nossos).

Na onda das denúncias ao software, a transparência, as escolhas dos Estados compradores de tecnologia devem ser motivadas, seja para as contas públicas ou para realizar o accountability exigido pela sociedade civil. Casos como o da licitação uruguaia e as contratações desprovidas de qualquer exigência técnica realizadas junto à ETICE não devem se repetir. O direito à autodeterminação do uso dos dados estende os seus efeitos ao direito de informação quanto aos sistemas de reconhecimento facial adquiridos e os seus índices de desempenho. O acesso às informações mínimas figura como direito do cidadão.

Nesse sentido, ao estabelecer uma finalidade delimitada para o uso das tecnologias de videomonitoramento, são traçados os limites para a coleta predatória de imagens e a venda dos *templates* no lucrativo comércio do capitalismo de vigilância (Zuboff; Bruno, 2018).

Ao ter consciência dos algoritmos utilizados e seus respectivos bancos de imagens, a sociedade civil pode enfim passar a assumir o papel de protagonismo na autodeterminação do uso de seus dados. Seja ao acompanhar os perfilamentos que contenham informações suas, ou até mesmo na proposição de denúncias a algoritmos que possuem vieses injustificáveis para pessoas negras e mulheres.

Por meio da transparência e divulgação de informações básicas, até mesmo a teia de matemática estatística da rede neural passa a fazer sentido e ser passível de questionamentos.

REFERÊNCIAS BIBLIOGRÁFICAS

ABBAS DA SILVA, L.; FRANQUEIRA, B. D.; HARTMANN, I. A. O que os olhos não veem, as câmeras monitoram: reconhecimento facial para segurança pública e regulação na América Latina. **Revista Digital de Direito Administrativo**, [S. l.], v. 8, n. 1, p. 171-204, 2021. DOI: 10.11606/issn.2319-0558.v8i1p171-204. Disponível em: https://www.revistas.usp.br/rdda/article/view/173903. Acesso em: 26 ago. 2023.

ACCESS NOW. T**ecnologia de vigilância na América Latina: Feita no exterior, implantada em cas**. Access Now Org, 2021. Disponível em; https://www.accessnow.org/wp-content/uploads/2021/08/vigilancia-latam-port.pdf . Acesso em: 04 fev. 2025.

AMORES, Yessica Santos de. RECONOCIMIENTO FACIAL CON FINES DE SEGURIDAD PÚBLICA EN URUGUAY. ANÁLISIS DESDE LA PERSPECTIVA DE LA ORGANIZACIÓN ADMINISTRATIVA. **Revista Derecho Público**, [S.l.], n. 60, p. 111 - 127, june 2022. ISSN 2301-0908. DOI: https://doi.org/10.31672/60.5. Disponível em: <https://www.revistaderechopublico.com.uy/ojs/index.php/Rdp/article/view/170>. Acesso em: 07 fev. 2025.

ANDRÉA, G. F. M.; SILVA, D. C. da; GUNDIM, W. W. D. TECNOLOGIA DE RECONHECIMENTO FACIAL COMO POLÍTICA DE SEGURANÇA PÚBLICA: O CASO DO METRÔ DE SÃO PAULO. **Revista da Faculdade de Direito do Sul de Minas**, [S. l.], v. 38, n. 2, p. 279–298, 2022. Disponível em: https://revista.fdsm.edu.br/index.php/revistafdsm/article/view/376. Acesso em: 9 jan. 2025.

ARAÚJO, Letícia de Sousa. Entre holofotes e fracassos: a experiência do Programa Ronda do Quarteirão no Ceará. **Revista Brasileira de Segurança Pública**, [S. l.], v. 13, n. 1, p. 76–94, 2019. DOI: 10.31060/rbsp.2019.v13.n1.1059. Disponível em: https://revista.forumseguranca.org.br/rbsp/article/view/1059. Acesso em: 24 nov. 2024.

ASOCIACIÓN POR LOS DERECHOS CIVILES. **Tu yo digital. Descubriendo las narrativas sobre identidad y biometría en América Latina: los casos de Argentina, Brasil, Colombia y México**. ADC, 2019.Disponible en: https://adc.org.ar/wp-content/uploads/2020/06/050-tu-yo-digital-04-2019.pdf. Acesso em: 18 nov. 2024.

AUF. TV. **Video demostrativo del sistema de cámaras de identificación facial**. Duração: 0:25. Publicado em 31 de março de 2017. Disponível em: https://www.youtube.com/watch?v=B5_awfmlQOU. Acesso em: 22 dez. 2024.

BIONI, Bruno Ricardo; LUCIANO, Maria. **O princípio da precaução na regulação de inteligência artificial : seriam as leis de proteção de dados o seu portal de entrada?**. in. Inteligência artificial e direito : ética, regulação e responsabilidade (Livro) São Paulo : Revista dos Tribunais, 2019. (2019), p. 207-231.

BOURDIEU, Pierre. **A distinção: crítica social do julgamento**. São Paulo: Edusp, 2007.

BRANDÃO, Diogo Alves. **Inteligência Artificial e Aprendizado de Máquina: da teoria ao algoritmo pronto no Ensino Médio**. 2023- 105 p. Dissertação de Mestrado-Departamento de Matemática- Universidade de Brasília- UnB- Brasília, 2023.

BRUNO, Fernanda. **Visões Maquínicas Da Cidade Maravilhosa: Do Centro De Operações Do Rio À Vila Autódromo**. In: Tecnopolíticas da vigilância : perspectivas da margem / organização Fernanda Bruno ... [et al.] ; [tradução Heloísa Cardoso Mourão ... [et al.]]. - 1. ed. - São Paulo: Boitempo, 2018.

BUOLAMWINI, Joy. U**nmasking AI: My Mission to Protect What Is Human in a World of Machines**. New York. Penguin Random House, 2023.

CARNEIRO, Fernanda Vaz Borges; COSTATO, Liz Carolina Jaber. **Avaliando o impacto das modificações faciais voluntárias em modelos de aprendizagem profunda no reconhecimento facial** / Fernanda Vaz Borges Carneiro; Liz Carolina Jaber Costato; orientador Flávio Barros Vidal. -- Brasília, 2023.113p.Projeto Final de Curso (Engenharia de Controle e Automação) -- Universidade de Brasília, 2023.

CATAI, Henrique; REJOWSKI, Mirian. **Violência e turismo na imprensa brasileira– matérias da Folha de S. Paulo (1990 a 2000)**. Anais... II Seminário de Pesquisa em Turismo do Mercosul, set, 2004.

COSTA, Paula Cristina Santos. Política criminal atuarial e controle urbano: a representação do bairro - do onde - como elemento justificador para ações repressivas do Estado. **Revista Latino-Americana de Criminologia**, [S. l.], v. 1, n. 1, p. 68–88, 2021. Disponível em: https://periodicos.unb.br/index.php/relac/article/view/37128. Acesso em: 28 jan. 2025.

DANTAS, Eustógio Wanderley Correia. **CONSTRUÇÃO DA IMAGEM TURÍSTICA DE FORTALEZA/CEARÁ**. Mercator, Fortaleza, v. 1, n. 1, jan. 2009. ISSN 1984-2201. Disponíve em: http://www.mercator.ufc.br/mercator/article/view/195>. Acesso em: 19 nov. 2024.

DA SILVA MORAES, Daniel. **Análise quantitativa da influência de degradações em modelos de aprendizagem profunda utilizados no Reconhecimento Facial**. Orientador Prof. Dr. Flávio de Barros Vidal. -- Brasília, 2023.92p. Projeto Final de Curso (Engenharia da Computação) - Universidade de Brasília, 2023.

DUARTE, Daniel Edler. (2024). Tecnopolíticas da falha: dispositivos de crítica e resistência a novas ferramentas punitivas. **Revista Brasileira de Ciências Sociais**. 39. 10.1590/39017/2024.

DUARTE, Evandro C. Piza. **Uma dogmática processual penal em crise ou uma dogmática para a crise do processo penal?** 2017. Prefácio ao livro de Rafael de Deus Garcia: Tecnologia e gestão da prova nos crimes de drogas. Editora D´Plácido, 2017.

DUARTE, Evandro C. Piza; MURARO, Mariel; et al. **Quem é o Suspeito do Crime de Tráfico de Drogas? Anotações sobre a dinâmica dos Preconceitos Raciais e Sociais na Definição das Condutas de Usuário e Traficante pelos Policiais Militares nas Cidades de Brasília, Curitiba e Salvador. in Coleção Pensando a Segurança Pública, Volume 5: Segurança Pública e Direitos Humanos: Temas Transversais.** Ministério da Justiça, Brasília: 2014. Disponível em :https://www.gov.br/mj/pt-br/assuntos/sua-seguranca/seguranca-publica/analise-e-pesquisa/download/estudos/pspvolume5/quem_suspeito_crime_traficos_droga.pdf. Acesso em: 8 set. 2024.

ELIAS, D; PEQUENO, R. **Reestruturação econômica e nova economia política da urbanização no Ceará**. Mercator, Fortaleza, v. 12, n. 28, mai./ago. 2013. p. 95-112. Disponível em: https://repositorio.ufc.br/bitstream/riufc/12354/1/2013_art_lrbpequeno.pdf. Acesso em: 8 nov. 2024.

ETICE, Empresa de Tecnologia da Informação do Ceará. **Manual de Serviços da Etice**. Etice.Ce. Disponível em: https://www.etice.ce.gov.br/wp-content/uploads/sites/5/2025/01/Manual-de-servicos-Etice-para-site.pdf . Acesso em 09 fev. 2025.

GONÇALVES FELIZ, Ana Beatriz; DUARTE, Evandro Charles Piza. Dilemas do uso da Tecnologia de Reconhecimento Facial: O caso do Uruguai e o uso do reconhecimento facial na segurança pública desportiva como vitrine tecnológica. **Revista Latino-Americana de Criminologia**, [S. l.], v. 4, n. 2, p. 181–226, 2024. Disponível em: https://periodicos.unb.br/index.php/relac/article/view/56279. Acesso em: 31 jan. 2025.

GARCIA, Rafael de Deus. **Tecnologia e gestão da prova nos crimes de drogas**. Editora D´Plácido, 2017.

GARCIA, Rafael de Deus; GONTIJO, Rogério Bontempo Cândido. Algoritmos e segurança pública: controle e vigilância no policiamento baseado em dados. **Revista Latino-Americana de Criminologia**, [S. l.], v. 1, n. 1, p. 14–43, 2021. Disponível em: https://periodicos.unb.br/index.php/relac/article/view/36735. Acesso em: 4 fev. 2025.

GOB.UY. **Cámaras de reconocimiento facial erradicaron episodios violentos en el fútbol Uruguay Presidencia. Subsecretário Jorge Vázquez**. Atualizado em 23/08/2018. Disponível em:https://www.gub.uy/presidencia/comunicacion/noticias/camaras-reconocimiento-facial-erradicaron-episodios-violentos-futbol . Acesso em: 24 jan. 2025.

GOVERNO DO ESTADO DO CEARÁ. **Ceará contra o Crime: Estado vai realizar novos concursos e implementar reconhecimento facial e rastreamento de motos**. Ceará. Gov: Segurança Pública. Editada em 26 de agosto de 2024. Acesso em: 24 nov. 2024.

FAGUNDEZ, Fabrício. **Desarrollo de programas basados en la Inteligencia Artificial para la predicción del delito**. 2023 in Portada: Revista de la Dirección Nacional de la Educación Policial. Año I – N.º 1- Diciembre de 2023 - Publicación anual. Org.Comisario General (R) Roberto de los Santos.

FERNÁNDEZ, Robert García. Análisis de los diferentes abordajes de investigación aplicados a la identificación Criminal. Estudio de la aplicabilidad de nuevas estrategias de acción:

"Reconocimiento Facial".2022 in Portada: **Revista de la Dirección Nacional de la Educación Policial**. Año I – N.º 1- Diciembre de 2023 - Publicación anual. Org.Comisario General (R) Roberto de los Santos.

FERREIRA, D. L. de S.; NOVAES, S. M. de; MACEDO, F. G. L. **Cidades inteligentes e inovação: a videovigilância na Segurança Pública de Recife, Brasil**. Cadernos Metrópole, [S. l.], v. 25, n. 58, p. 1095–1122, 2023. DOI: 10.1590/2236-9996.2023-5814. Disponível em: https://revistas.pucsp.br/index.php/metropole/article/view/59793. Acesso em: 10 jan. 2025.

FIRMINO, Rodrigo José. **Securitização, vigilância e territorialização em espaços públicos na cidade neoliberal**. 2017. In: Tecnopolíticas da vigilância : perspectivas da margem / organização Fernanda Bruno ... [et al.] ; [tradução Heloísa Cardoso Mourão ... [et al.]]. - 1. ed. - São Paulo : Boitempo, 2018.

GAGNE, David. **'Barras Bravas' en Uruguay se han transformado en carteles: funcionario**. InSight. Crime. Publicado em 25 de abril de 2017. Disponível em:https://insightcrime.org/es/noticias/noticias-del-dia/barras-bravas-uruguay-transformado-carteles-delegado-asociacion-futbolistica/. Acesso em: 05 fev. 2025.

HAYON, Alejandra. S**eis días arrestado por un error del sistema de reconocimiento facial**. Página 12; El país, 2019. Disponível em;https://www.pagina12.com.ar/209910-seis-dias-arrestado-por-un-error-del-sistema-de-reconocimien. Acesso em: 19 de set. 2023.

HUGO, Victor. **Trabalhadores do Mar**. Trad. Machado de Assis. Abril Cultural. 1ª Edição, Julho- 1971.

JÚNIOR, Benedito Maciel da Silva. **O impacto da criminalidade na demanda turística do nordeste brasileiro**. 2017. 36f. - Dissertação (Mestrado) - Universidade Federal do Ceará, Programa de Economia Profissional, Fortaleza (CE), 2017. Disponível em: https://repositorio.ufc.br/handle/riufc/28975. Acesso em: 5 fev. 2025.

LEE, Kai-Fu. **Inteligência artificial [recurso eletrônico] : como os robôs estão mudando o mundo, a forma como amamos, nos relacionamos, trabalhamos e vivemos** / Kai-Fu Lee ; tradução Marcelo Barbão.- 1. ed. - Rio de Janeiro : Globo Livros, 2019. recurso digital.

LYON, David. **Cultura da vigilância: envolvimento, exposição e ética na modernidade digital**. Trad. Heloísa Cardoso Mourão. 2017. In: Tecnopolíticas da vigilância : perspectivas da margem / organização Fernanda Bruno ... [et al.] ; [tradução Heloísa Cardoso Mourão ... [et al.]]. - 1. ed. - São Paulo: Boitempo, 2018.

MONTEVIDEU, UY. Viol**encia en el fútbol: ¿cuál es el rol del evaluador de seguridad que estará en tribunas?** Montevideu.uy: deportes, 2024. Disponível em: https://www.montevideo.com.uy/Deportes/Violencia-en-el-futbol--cual-es-el-rol-del-evaluador-de-seguridad-que-estara-en-tribunas--uc881192. Acesso em: 01 fev. 2025.

MINISTERIO DE ECONOMÍA Y FINANZAS, UY. **¿Qué es el Presupuesto Nacional?** Ministerio de Economía y Finanzas.uy: Presupuesto 2020-2024. Disponível em:https://www.gub.uy/ministerio-economia-finanzas/comunicacion/publicaciones/es-presupuesto-nacional. Acesso em: 02 fev. 2025.

ORTEGA.Simon Lopez. **El complejo problema de las barras bravas en Uruguay**. La Mañana.Uy. Atualizado em 10 de fevereiro de 2022. Disponível em: https://www.xn--lamaana-7za.uy/actualidad/el-complejo-problema-de-las-barras-bravas-en-uruguay/. Acesso em: 05 de fevereiro de 2025.

ORWELL, George. **A Revolução dos Bichos**. Rio de Janeiro: Companhia das Letras, 2009.

PAIVA, R. A. Urbanização e políticas de turismo no Ceará, Brasil. **Revista Turismo & Desenvolvimento**, n.21/22, p. 305-18, 2014. Disponível em https://repositorio.ufc.br/bitstream/riufc/9263/1/2014_art_rapaiva.pdf. Acesso em: 8 nov. 2024.

RIBEIRO, Marcelo da Silva. **"Do Tecnosolucionismo ao Tecnovigilantismo": Um estudo sociológico sobre os usos de emergentes tecnologias pelas forças de segurança do Ceará** / Marcelo da Silva Ribeiro. – 2024. 350 f. : il. color. Tese (doutorado) – Universidade Federal do Ceará, Centro de Humanidades, Programa de Pós-Graduação em Sociologia, Fortaleza, 2024.

ROUVROY, Antoinette; BERNS, Thomas. **Governamentalidade algorítmica e perspectivas de emancipação: o díspar como condição de individuação pela relação?.** 2013. Trad.Pedro Henrique Andrade. In: Tecnopolíticas da vigilância : perspectivas da margem / organização Fernanda Bruno... [et al.]; [tradução Heloísa Cardoso Mourão... [et al.]]. - 1. ed. - São Paulo: Boitempo, 2018.

SCHERCH, Vinicius Alves. **Impactos do Capital no Controle da Pauta Política na Era Pós-Digital**. Orientador: Prof. Dr. Vinício Carrilho Martinez/Coorientador: Dr. Carlos Eduardo Montes Netto. 2024. Tese (Doutorado em Ciência, Tecnologia e Sociedade)- Universidade Federal de São Carlos, São Carlos, 2024.

SCOGNAMIGLIO. Maria Eugenia. **Una vieja guerra narco: el homicidio del barra brava de Peñarol que la Policía aclaró nueve años después**. El Observador. Publicado em 08 de março de 2024. Disponível em: https://www.elobservador.com.uy/nota/una-vieja-guerra-narco-el-homicidio-del-barra-brava-de-penarol-que-la-policia-aclaro-nueve-anos-despues-202438113953. Acesso em: 05 fev. 2025.

SILVA, Marina Cavalli Ribeiro da. **A coleta de dados biométricos e a violação do direito fundamental à privacidade à luz da Lei Geral de Proteção de Dados Pessoais** / Marina. Cavalli Ribeiro da Silva. -- Franca, 2023. 130 p. Dissertação (mestrado) - Universidade Estadual Paulista (Unesp), Faculdade de Ciências Humanas e Sociais, Franca. Orientadora: Luciana Lopes Canavez.

SGSP. **El Sistema de Gestión de Seguridad Pública del Ministerio del Interior de la República Oriental del Uruguay. Serie de publicaciones sobre buenas prácticas para la calidad estadística, Centro de Excelencia para Información Estadística de Gobierno, Seguridad Pública, Victimización y Justicia de la Oficina de las Naciones Unidas contra la Droga y el Delito**, 2020. Disponível em: https://www.gub.uy/ministerio-interior/comunicacion/publicaciones/sistema-gestion-seguridad-publica-del-ministerio-del-interior-evaluacion. Acesso em: 23 dez. 2024.

SNOW, Jacob. **Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots**, ACLU (July 26, 2018) Disponível em: https://www.aclu.org/blog/privacytechnology/surveillance-technologies/amazons-face-recognition-falsely-matched-28 [perma.cc/PL69-FWQL]. Acesso em: 15 nov. 2024.

SOUZA, Nicolle Bêtta de; ACHA, Fernanda Rosa. A PROTEÇÃO DE DADOS COMO DIREITO FUNDAMENTAL: UMA ANÁLISE A PARTIR DA EMENDA CONSTITUCIONAL 115/2022. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, [S. l.], v. 8, n. 9, p. 666–684, 2022. DOI: 10.51891/rease.v8i9.6822. Disponível em: https://periodicorease.pro.br/rease/article/view/6822. Acesso em: 01 fev. 2025.

SECRETARIA DE SEGURANÇA PÚBLICA E DEFESA SOCIAL. **Crimes Violentos Letais Intencionais, CVLI: Estatística anual 2009 a 2024**. Secretaria de Segurança Pública e Defesa Social: estatísticas. Disponível em:https://www.sspds.ce.gov.br/wp-content/uploads/sites/24/2025/01/CVLI-Anual.pdf. Acesso em: 07 fev. 2025.

SECRETARIA DE SEGURANÇA PÚBLICA E DEFESA SOCIAL. **Fortaleza encerra 2023 com redução de 13,2% nas mortes por crimes violentos**. Policia Civil Ceará: SSDPS. Publicado em 09 de janeiro de 2024. Disponível em: https://www.policiacivil.ce.gov.br/2024/01/09/fortaleza-encerra-2023-com-reducao-de-132-nas-mortes-por-crimes-violentos-no-ceara-indicador-empata-com-2022/#:~:text=Fortaleza%20encerrou%20o%20ano%20de,contra%20850%20registros%20em%202022. Acesso em: 07 fev. 2025.

SUBRAYANDO. **El plan piloto que anunció Heber con inteligencia artificial en cámaras para prevenir delitos**. SUBRAYANDO: Policiales. Inteligencia Artificial. Atualizado em 10/10/2023. Disponível em: https://www.subrayado.com.uy/el-plan-piloto-que-anuncio-heber-inteligencia-artificial-camaras-prevenir-delitos-n928048 . Acesso em 21 dez. 2024.

VENTURINI, Jamila; GARAY, Vladimir. **Reconhecimento facial na América Latina:Tendências na implementação de uma tecnlogia perversa**. Consórcio Al Sur, 2021. Disponível em: https://www.alsur.lat/sites/default/files/202110/ALSUR_Reconocimiento%20facial%20en%20Latam_PR_Final.pdf. Acesso em: 15 nov. 2024.

WIENER. Norbert. **Cibernética e Sociedade o Uso Humano de Seres Humanos**. Tradução de JOSÉ PAULO PAES, 2a edição. EDITORA CULTRIX, São Paulo, 1968.

WU, Xun. **Guia de políticas públicas: gerenciando processos** / Xun Wu, M. Ramesh, Michael Howlett, Scott Fritzen; traduzido por Ricardo Avelar de Souza. – Brasília: Enap, 2014.

ZUBOFF, Shoshana. **Big Other: capitalismo de vigilância e perspectivas para uma civilização de informação**. 2015. Trad. Antonio Holzmeister Oswaldo Cruz e Bruno Cardoso. In: Tecnopolíticas da vigilância : perspectivas da margem / organização Fernanda Bruno ... [et al.] ; [tradução Heloísa Cardoso Mourão ... [et al.]]. - 1. ed. - São Paulo: Boitempo, 2018.

MARCO LEGISLATIVO

Asunto 147701. CSS 330/2020.388/0. Presupuesto Nacional 2020-2024. Disponible en url: https://parlamento.gub.uy/documentosyleyes/documentos/versiones-taquigraficas/senadores/49/388/0/HTM.

Asunto 147701. CSS 330/2020.394/0. Presupuesto Nacional 2020-2024. Disponible en url: https://parlamento.gub.uy/documentosyleyes/documentos/versiones-taquigraficas/senadores/49/394/0/HTM.

URUGUAY. CÓDIGO PENAL Nº 9.155.Actualización de la Versión Oficial publicada el 26.10.1967 (Decreto Nº 698/967).

URUGUAY.DECRETO Nº 14762. Determinación que la Identificación de las Personas Fisicas, de das Empresas y de los Empresarios se Ajustará a las Reglas que se Determina Poder Ejecutivo, Consejo de Ministros. Publicado em 13/02/1978. Diaro Oficial de la Republica Oriental del Uruguay. Montevidéo, Lunes 20 de Febrero de 1973.

URUGUAY.DECRETO Nº 387/016.Apruébase el Anexo I elaborado por el Ministerio del Interior, que contiene las medidas a aplicar en los eventos deportivos. Poder Ejecutivo, Consejo de Ministros. Publicado em 21/12/2016. Diaro Oficial de la Republica Oriental del Uruguay. Montevidéo, Documentos, 21 deciembre de 2016.

URUGUAY.DECRETO Nº 01/021. Reglamentacion del Art. 1 Bis de la Ley 19.534, Relativa a la Creacion de un Registro de Personas Impedidas de Ingresar a Espectaculos Publicos. Poder Ejecutivo, Consejo de Ministros. Publicado em 05/01/2021. Diaro Oficial de la Republica Oriental del Uruguay. Montevidéo, Documentos, 12 enero de 2021.

URUGUAY. LEY Nº 18.331:Ley de Protección de Datos Personales. Publicada no dia 18/08/2008. Registro Nacional de Leyes y Decretos. Diaro Oficial de la Republica Oriental del Uruguay. Montevidéo, Documentos, 18 agosto de 2008.

URUGUAY. DECRETO Nº 232/010: Reglamentación de la Ley sobre el Derecho de Acceso a la Información Pública. Publicada no dia 10/08/2010. Registro Nacional de Leyes y Decretos. Diaro Oficial de la Republica Oriental del Uruguay. Montevidéo, Documentos, 10 agosto de 2010.

URUGUAY. LEY Nº 19.315: Aprobación de la Ley Organica Policial. Poder Ejecutivo, Ministerio del Interior. Publicada no dia 24/02/2015. Registro Nacional de Leyes y Decretos. Diaro Oficial de la Republica Oriental del Uruguay. Montevidéo, Documentos, 24 febrero de 2015.

BRASIL. Constituição (1988) . Constituição da República Federativa do Brasil: promulgada em 5 de outubro de 1988. Diário Oficial da União de 05 out de 1988.

BRASIL. Lei Geral de Proteção de Dados Pessoais-Lei nº 13.709, de 14 de Agosto de 2018. Brasília, DF: Congresso Nacional, 2018. Diário Oficial da União de 15 ago de 2018

BRASIL. Ministério da Justiça e Segurança Pública. Gabinete do Ministro. Portaria nº 793, de 24 de outubro de 2019. Brasília, 2019. Diário Oficial da União de 25 out de 2019.

DOCUMENTOS REFERENTES ÀS LICITAÇÕES E JURISPRUDÊNCIA

URUGUAY. LICITACIÓN PÚBLICA 13/2019**.** Ministerio del Interior: Secretaría del Ministerio del Interior.

BRASIL. Edital nº 2021/11860. Superintendência da Policia Civil.

BRASIL.Edital nº 20230021.Superintendência da Policia Civil.

TRIBUNAL DE APELACIONES CIVIL. Sentencia Definitiva Nº 15/2023. 1º Turma Civil. Redatora Min. Dra Beatriz Venturini. Publicação em 08/02/2023.