



O USO DE RECONHECIMENTO FACIAL PARA FINS DE SEGURANÇA PÚBLICA: UMA ANÁLISE DO CASO “SMART SAMPA”

Giovanna de Albuquerque Barbosa (Bolsista) e Eduardo Altomare Arienti (Orientador)

Apoio: PIBIC CNPq

RESUMO

Diante das inovações tecnológicas, em que ocorre o uso da inteligência artificial de reconhecimento facial para fins de segurança pública, se faz necessária a regulamentação dessa tecnologia, buscando dirimir potenciais impactos nos direitos fundamentais que são garantidos pela Constituição Federal brasileira. O projeto denominado “Smart Sampa” traz à luz da pesquisa elementos importantes para analisar a problemática acerca da implementação de novas tecnologias no Brasil. Tal caso trata-se de uma iniciativa realizada pela Prefeitura de São Paulo, que faz a implementação de câmeras com o sistema de reconhecimento facial, em que uma das finalidades do projeto é a eficiência dos serviços de segurança pública, entre outros fins. Dada a novidade do tema, o projeto “Smart Sampa” gerou preocupações por parte dos operadores do direito e, por conseguinte, a discussão foi levada para apreciação do Poder Judiciário, uma vez que a implementação de sistemas de reconhecimento facial demonstrou riscos aos direitos fundamentais constitucionais, devido ao fato de ainda não haver uma legislação de inteligência artificial no Brasil, especificamente, para sistemas de reconhecimento facial. Desta forma, a regulamentação prévia à implementação dessa tecnologia é elemento crucial para proteger os direitos fundamentais das pessoas, evitando possíveis violações de tais direitos e, concomitantemente, propiciando o desenvolvimento e a inovação tecnológica de forma segura e eficaz.

Palavras-chave: Reconhecimento Facial. Direitos Fundamentais. Políticas de Segurança Pública.

ABSTRACT

In the face of technological innovations involving the use of artificial intelligence for facial recognition purposes in public security, there is a pressing need for the regulation of this technology to address potential impacts on fundamental rights guaranteed by the Brazilian Federal Constitution. The project known as "Smart Sampa" brings important elements to the research in order to analyze the issues surrounding the implementation of new technologies in Brazil. This initiative, carried out by the São Paulo City Hall, involves the deployment of cameras equipped with facial recognition systems, with one of the project's goals being the enhancement of public security services, among other objectives. Given the novelty of the



subject, the "Smart Sampa" project has raised concerns among legal practitioners, leading to judicial review, as the implementation of facial recognition systems has demonstrated risks to constitutional fundamental rights. This is due to the absence of specific artificial intelligence legislation in Brazil, particularly concerning facial recognition systems. Therefore, prior regulation of this technology is crucial to protect individuals fundamental rights, preventing possible violations, while concurrently fostering technological development and innovation in a secure and effective manner.

Keywords: Facial Recognition; Fundamental Rights; Public Security Policies.



1. INTRODUÇÃO

O projeto “Smart Sampa” tem como objetivo a implementação de câmeras instaladas pela Prefeitura de São Paulo, que fazem o uso da inteligência artificial de reconhecimento facial com a capacidade de identificar pessoas. Especialmente, tal projeto tem como finalidade trazer melhorias nos serviços de segurança pública, por meio de uma Central de Monitoramento, integrando as ações da CET, SPTrans, CPTM, Metrô, SAMU, Guarda Civil Metropolitana e Polícia Militar.

A implementação de sistemas de reconhecimento facial tem sido alvo de discussões judiciais, dada a probabilidade de violação de direitos fundamentais. Os direitos que podem ser violados são a presunção de inocência, o direito de liberdade e de locomoção, o direito à privacidade, o direito à proteção de dados pessoais, entre outros, todos garantidos pela Constituição Federal do Brasil.

Um exemplo da judicialização no que concerne ao uso de reconhecimento facial em espaços públicos é o caso da Companhia do Metropolitano de São Paulo. Com a propositura de Ação Civil Pública pela Defensoria Pública do Estado de São Paulo, em que há a acusação de diversas possíveis violações de direitos fundamentais. Em 22 de março de 2022, o Tribunal de Justiça de São Paulo concedeu a liminar para barrar o uso de reconhecimento facial, nesses termos, decidiu a 6ª Vara de Fazenda Pública:

Assim, sopesando as consequências, de rigor a concessão da liminar para impedir a execução do sistema de captação e tratamento de dados biométricos dos usuários de metrô para sua utilização em sistemas de reconhecimento facial, admitindo-se apenas a instalação. A partir da publicação desta decisão estará correndo o prazo para o Metrô apresentar contestação (BRASIL, 2022, p. 1587).

Com relação ao projeto “Smart Sampa”, ocorreu a propositura de Ação Popular em face da Prefeitura Municipal de São Paulo, questionando a legitimidade jurídica do projeto. A decisão de suspensão do pregão que visava à contratação de serviços de reconhecimento facial, pela 3ª Vara de Fazenda Pública do Tribunal de Justiça de São Paulo, em 18 de maio de 2023, acompanha o racional de proteção primordial dos direitos fundamentais.

Diante desse contexto, na ausência de uma regulação legal, em especial prévia à implementação do projeto almejado, diviso verossimilhança do direito postulado e grave ameaça a direitos fundamentais acima mencionados e determino a suspensão provisória do pregão indicado no pedido da petição inicial (BRASIL (b), 2023, p. 459).

Nesse sentido, são possíveis as violações de direitos fundamentais que decorrem do uso dessa tecnologia. De acordo com o InternetLab, centro independente de pesquisa interdisciplinar e que colaborou com um parecer técnico que analisa o uso de sistemas de reconhecimento facial pela Companhia do Metropolitano de São Paulo, essa ferramenta está inevitavelmente sujeita a erro, uma vez que os erros são componentes básicos do funcionamento dessa tecnologia.

A acurácia desse tipo de sistema, portanto, é resultado da calibração das ocorrências de falsos positivos e falsos negativos. Isso tem como consequência uma característica intrínseca ao tipo de mecanismo aqui analisado: a impossibilidade de que o sistema opere sem nenhum tipo de falha, tendo em vista que a existência de erros é componente básico de seu funcionamento. Nesse contexto, é relevante ainda destacar que o aumento da acurácia não resolve, por si só, os problemas relacionados à implementação do uso de reconhecimento facial – o que será exposto em outros tópicos deste parecer, como aquele que discorre sobre vieses raciais no uso dessas tecnologias (ABELLO; ARAÚJO; HIRATA JR, 2023, p. 28).

Sendo assim, em razão da possibilidade de erros inerentes ao sistema de reconhecimento facial e diante da possibilidade de se atingir direitos fundamentais, é imprescindível a adesão de boas práticas na implementação de novas tecnologias, visando dirimir potenciais violações de direitos fundamentais, sobretudo com o uso transparente dessa ferramenta e com expresse respaldo legal, por meio de regulamentação específica.

Posto isso, será feito um estudo nos próximos tópicos desta pesquisa, a fim de compreender como é o funcionamento de sistemas de reconhecimento facial, em que será demonstrada a ocorrência de falsos positivos e falsos negativos, bem como outros parâmetros materiais e que compõem a tecnologia em si, com o intuito de evidenciar como essa tecnologia é passível de erro, problematizando-a. Tal estudo terá como base artigos feitos por especialistas que descrevem essas falhas.

Ainda, será demonstrado como o conflito entre políticas de segurança pública e direitos fundamentais existe na prática, ao analisar o projeto “Smart Sampa”, bem como o porquê tal projeto fomentou discussões judiciais. Além da análise das consequências da implementação dessa tecnologia, serão demonstrados, ao decorrer da pesquisa, quais os efeitos do uso de reconhecimento facial para fins de segurança pública, quando não decorrem de prévia regulamentação.

Outrossim, para a investigação dos efeitos dessa tecnologia na sociedade, serão apresentados casos concretos de violação de direitos fundamentais, que provam como esse instrumento foi utilizado de forma prejudicial e em desacordo com os direitos fundamentais,



por meio de notícias jornalísticas que narram esses casos, bem como artigos que exploram o tema e processos judiciais que discutem essa matéria.

Ao observar as consequências da utilização de sistemas de reconhecimento facial para fins de segurança pública, é possível determinar como a regulamentação prévia do uso dessa tecnologia é crucial para a sua posterior implementação. Com suporte do entendimento jurídico a respeito do tema, é viável concluir, concomitantemente, como possibilitar a coexistência entre a garantia de direitos fundamentais e políticas de segurança pública que utilizam dessa ferramenta e, conseqüentemente, propiciam o exercício da inovação tecnológica.

Dessa forma, com o objetivo de compreender como o tema vem sendo discutido em aspectos jurídicos, a pesquisa observará pontos relevantes de como se dará a regulamentação no Brasil e em outros países, bem como analisará os processos judiciais que discutem o uso de reconhecimento facial como método de segurança pública e, ainda, trará referências que exploram a importância da garantia de direitos fundamentais nos atos dos poderes públicos.

2. SISTEMA DE RECONHECIMENTO FACIAL E AS PROBLEMÁTICAS RELATIVAS AO SEU FUNCIONAMENTO E IMPLEMENTAÇÃO

Como supramencionado, o uso do sistema de reconhecimento facial pela Prefeitura de São Paulo tem sido implementado com o propósito de melhorar a eficácia dos serviços públicos, integrando os sistemas de segurança para o monitoramento da cidade. De acordo o artigo feito pelos autores Fabio Faria, Raoni Teixeira e Rafael Januzi, o sistema de reconhecimento facial se baseia na análise de imagens por meio de um sistema comparativo para a identificação de pessoas.

Mais precisamente, um sistema de RF é composto por algoritmos que analisam as fotos dos rostos e extraem um conjunto de características distinguíveis. As características correspondem aos atributos físicos da face como, por exemplo, as distâncias entre os olhos e o formato do nariz e, em geral, são codificadas em um objeto denominado template. Os templates são armazenados em uma base de dados para comparações futuras. A correspondência entre faces é calculada por um algoritmo que verifica a semelhança entre templates. O resultado da comparação é um número real chamado de score (pontuação). Quanto maior esse número, mais semelhantes são as pessoas (TEIXEIRA; JANUZI; FARIA, 2023, p. 5).

Dessa maneira, uma vez definido em linhas gerais como funciona o sistema de reconhecimento facial, restam dois parâmetros de funcionamento a serem analisados: a verificação e a identificação. Conforme o parecer técnico do InternetLab, a verificação é a comparação entre duas imagens, em que o resultado é a decisão de se as imagens correspondem à mesma pessoa, ou não; enquanto a identificação é realizada pela análise de uma lista de imagens associadas a identidades conhecidas, a tarefa do algoritmo é analisar uma nova imagem e compará-la (ABELLO; ARAÚJO; HIRATA JR, 2023).

Segundo evidências do mesmo parecer, há dois erros que podem decorrer da verificação ou identificação, os chamados “falsos positivos” ou “falsos negativos”. Os falsos positivos ocorrem quando o modelo associa incorretamente dois sujeitos, atribuindo a identidade de um sujeito a uma imagem que não lhe corresponde; já os falsos negativos ocorrem quando o modelo não reconhece que uma imagem corresponde a uma determinada identidade (ABELLO; ARAÚJO; HIRATA JR, 2023). Ademais, o tópico IV do parecer em questão discorre sobre outras falhas inerentes ao uso do sistema de reconhecimento facial, as limitações e principais causas da perda de performance da máquina, como a resolução da imagem, o envelhecimento e idade das pessoas.

Em razão da fase de desenvolvimento dessa tecnologia, o aperfeiçoamento da máquina se faz necessário, sobretudo antes de uma implementação em massa. Em uma perspectiva jurídica, o autor Ingo Wolfgang Sarlet expõe que “dentre os diversos desafios advindos com o aumento exponencial dos usos da IA sobressai o problema dos limites éticos e jurídicos da utilização das máquinas autônomas” (OLIVEIRA *apud* SARLET, 2022, p. 94) ou seja, além das questões técnicas, que compõem essa tecnologia passível de falhas, restam outras incertezas que demonstram a necessidade de um olhar mais atento com relação à implementação de sistemas de reconhecimento facial, que podem ser utilizados de forma imprópria.

A adoção generalizada de técnicas de reconhecimento facial tem levantado uma série de preocupações relacionadas com uso dessas tecnologias, principalmente em espaços públicos. Uma das preocupações é que essas tecnologias venham a ser utilizadas para restringir liberdades e monitorar e/ou perseguir grupos minoritários e políticos (TEIXEIRA; JANUZI; FARIA, 2023, p. 2).

Diante dessas adversidades, políticas internacionais já buscam estabelecer uma legislação específica para regular o uso dessa tecnologia. A título de exemplo, pode ser citada a nova Lei 2024/1689 de Inteligência Artificial, pioneira na Europa, aprovada pelo conselho europeu em 2024, que traz diversos pontos para auxiliar uma regulamentação segura e eficaz



e serve de exemplo para o resto do mundo, em especial no que diz respeito ao tratamento legal dos sistemas de reconhecimento facial.

3. GARANTIA DOS DIREITOS FUNDAMENTAIS NO ÂMBITO DOS ATOS DOS PODERES PÚBLICOS

Neste cenário de violações de direitos fundamentais, cumpre mencionar que esses direitos têm sua importância dado o contexto histórico em que surgiram, com o constitucionalismo e a limitação do poder do Estado, visando garantir a dignidade da pessoa humana e os direitos fundamentais do homem (SARLET; MARINONI; MITIDIERO, 2017). Assim sendo, os direitos fundamentais contidos na Constituição Federal do Brasil servem como alicerce para todo o ordenamento jurídico. O autor Ingo Wolfgang Sarlet, menciona em sua obra “A eficácia dos direitos fundamentais” racional importante que define os direitos fundamentais como normas direcionadoras.

Ao art. 5º, §1º, da Constituição de 1988 é possível atribuir, sem sobra de dúvidas, o mesmo sentido outorgado ao art. 18/1 da Constituição da República Portuguesa e ao art. 1º, inc. III da Lei Fundamental da Alemanha, o que, em última análise, significa – de acordo com a lição de Jorge Miranda – que cada ato (qualquer ato) dos poderes públicos deve tomar os direitos fundamentais como “baliza e referencial” (SARLET, 2009, p. 366).

Servindo os direitos fundamentais como baliza e referencial para os atos dos poderes públicos, esses têm como dever garantir tais direitos com afinco. A premissa é de que, para o caso em questão, a regulamentação prévia à implementação de novas tecnologias é garantia de que os poderes públicos percebem os direitos fundamentais como sendo elementos primordiais a serem observados, previamente a qualquer ato público.

Desse modo, quando os atos dos poderes públicos utilizam dos direitos fundamentais como baliza e referencial, buscando garantir tais direitos previamente a quaisquer atos públicos, consequentemente garantem a aplicabilidade imediata dessas normas. De acordo com o art. 5º, §1, da Constituição Federal de 1988, as normas que definem os direitos e garantias fundamentais são de aplicação imediata, nesse sentido, Ingo Wolfgang Sarlet argumenta que a aplicabilidade imediata dos direitos fundamentais requer uma juridicidade reforçada.

Nesse sentido, assume papel relevante a norma contida no art. 5º, § 1, da CF de 1988, de acordo com a qual todos os direitos e garantias fundamentais foram elevados à condição de normas jurídicas diretamente aplicáveis, e



portanto, capazes de gerar efeitos jurídicos. Apesar de inexistir norma constitucional destituída de eficácia jurídica, o fato é que o princípio da aplicabilidade imediata dos direitos fundamentais diferencia – no sentido de uma juridicidade reforçada (SARLET, 2009, p. 73).

No caso em questão, o princípio da aplicabilidade imediata dos direitos fundamentais só se tornará efetivo, na prática, por meio de normas que garantam tais direitos e que deverão estar dispostos em uma regulamentação de sistemas de inteligência artificial. Dessa maneira, viabilizando a implementação dessa tecnologia em prol da sociedade e não em desacordo com os direitos fundamentais, uma vez que esses direitos devem ser observados antes de quaisquer atos dos poderes públicos, garantindo a “juridicidade reforçada” desses direitos e garantias fundamentais.

3.1. Direito de liberdade de locomoção e a presunção de inocência

Cumpra salientar que para o autor José Afonso da Silva, o direito de liberdade consiste na “possibilidade de coordenação consciente dos meios necessários à realização da felicidade pessoal” (SILVA, 2017, p. 233), desse modo, dada a importância do direito de liberdade do homem, a Constituição Federal conceitua o direito de locomoção da pessoa física, sendo esse um mecanismo constitucional que opera em razão do direito de liberdade.

Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

XV – é livre a locomoção no território nacional em tempo de paz, podendo qualquer pessoa, nos termos da lei, nele entrar, permanecer ou dele sair com seus bens;

Nesse sentido, no Brasil, segundo índices do IBGE, há um tratamento desigual dos brasileiros com relação às questões raciais, “apesar de a população preta ou parda ser maioria no Brasil (55,8%), esse grupo, em 2018, representou apenas 27,7% das pessoas quando se consideram os 10% com os maiores rendimentos” (IBGE, 2019, p. 4). Logo, por uma questão relacionada à renda, o pressuposto é de que essa população é a mais dependente de serviços públicos, como por exemplo o transporte público, ou seja, exatamente aqueles serviços que são alvos do uso de reconhecimento facial como método de monitoramento em massa. Dito isso, essa tecnologia condiciona um tratamento desigual da população, principalmente em um país com diversos desafios que decorrem da desigualdade social, entre elas a racial e a



econômica.

Outrossim, estudos feitos por Buolawwivi e Gebru demonstram que a base de dados de reconhecimento facial tende a ser mais populadas por homens e indivíduos de tons mais claros de pele, por isso a performance dos classificadores é melhor para pessoas de tons de pele mais claros, que tendem a ser mais corretamente classificadas que pessoas de tom de pele escuro. Mulheres de tom de pele escuro são de forma unânime mais incorretamente classificadas, ademais, foram testados modelos na base de dados do MORFH-II, o estudo concluiu que afro-americanos têm maior probabilidade de serem confundidos entre si do que outros grupos (ABELLO; ARAÚJO; HIRATA JR, 2023).

Em acréscimo a essas evidências, de acordo com o parecer feito pelo Prof. Dr. Hirata Jr., que analisou os documentos na demanda judicial no caso da Companhia do Metropolitano de São Paulo, afirmou: “a potencialidade de o sistema perpetuar desigualdades presentes no Brasil, selecionando de maneira errada com maior frequência indivíduos negros e imigrantes” (BRASIL, 2022, p. 9). Além disso, a problemática não se limita ao funcionamento da máquina em si, uma vez que a implementação da tecnologia dependerá de quem é responsável por ela.

Nesse contexto, é relevante destacar que a popularização dos usos de reconhecimento facial na segurança pública traz especial preocupação em relação a questões raciais, diante da reprodução de racismo estrutural identificada por especialistas nas políticas públicas de segurança no Brasil. Isso porque há o risco de que o uso dessas tecnologias reproduza discriminações de natureza racial já existentes nos âmbitos nos quais elas são implementadas e, nesse contexto, a melhora na acurácia do sistema não resolve os problemas identificados, mas sim pode facilitar a perseguição de determinados grupos, uma vez que a implementação da tecnologia no mundo concreto depende também de escolhas de quem é responsável por gerir as políticas públicas (ABELLO; ARAÚJO; HIRATA JR, 2023, p. 59).

Na decisão judicial que suspendeu o pregão do “Smart Sampa”, o juiz competente argumenta com base em diversos estudos feitos por pesquisadores e instituições renomadas no Brasil e no exterior, afirmando que há riscos concretos no uso de sistemas de monitoramento por meio de reconhecimento facial, uma vez que a tecnologia reproduz padrões de discriminação e viabiliza a reprodução de racismo estrutural (BRASIL (b), 2023).

Tratando-se de casos concretos em que ocorre a violação de direitos fundamentais, é o caso de um homem negro que foi preso nos EUA e passou 10 dias na cadeia devido a uma falha do sistema de reconhecimento facial. Segundo a CNN Brasil, Nijeer Parks foi detido depois que o software da ClearView AI o identificou como um suspeito de roubo em New Jersey (SISTEMA, 2024). De acordo com o Instituto Igarapé, no Brasil, o uso de

reconhecimento facial no Estado do Rio de Janeiro, no ano de 2019, levou à detenção de uma mulher no bairro de Copacabana por conta de um falso positivo, em que o ocorrido levantou preocupações acerca do protocolo de abordagem tomado (VIDEOMONITORAMENTO, 2024).

Ademais, a petição inicial contra o edital do programa “Smart Sampa” faz menção à ocorrência de discriminação, bem como a violação ao direito de liberdade “assim, ante o todo exposto, resta também evidenciado que o Edital do “Smart Sampa”, ao utilizar a tecnologia do reconhecimento facial, fere a Constituição Federal nos termos acima aduzidos” (BRASIL (b), 2023, p. 18).

Por essas razões, a discriminação algorítmica inevitavelmente afeta o direito de igualdade, já que existem vieses raciais inseridos no funcionamento dessa tecnologia, e como consequência, acontece a violação do direito de liberdade de locomoção e da presunção de inocência, tidos como direitos fundamentais, conforme art. 5º, XV e LVII da Constituição Federal.

3.2. Direito à privacidade

O direito à privacidade é tido como direito fundamental e a Constituição Federal dispõe em seu art. 5º, inciso X que “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação”, posto isso, o cumprimento desse direito é ainda mais relevante no mundo contemporâneo, em razão do advento de novas tecnologias. Sob a perspectiva da doutrina, esse direito “conduz à pretensão do indivíduo de não ser foco da observação por terceiros, de não ter os seus assuntos, informações pessoais e características particulares expostas a terceiros ou ao público em geral” (MENDES; BRANCO, 2012, p. 411).

Em linhas gerais, o reconhecimento facial é tido como categorização biométrica, uma vez que os dados biométricos tornam possível a identificação do indivíduo. De acordo com a Lei nº 13.709/18, a Lei Geral de Proteção de Dados Pessoais (“LGPD”), em seu art. 5º, II, o dado biométrico é um dado pessoal sensível, sendo assim, a proteção de dados pessoais é um direito fundamental, em analogia ao disposto no art. 5º, X, da Constituição Federal. Reitera Ingo Wolfgang Sarlet: “que a despeito das interseções e articulações com outros direitos, fica assegurada à proteção de dados a condição de direito fundamental autônomo, com âmbito de proteção próprio” (SARLET, 2024).



Os argumentos trazidos pela Defensoria Pública da União, na Ação Civil Pública em face da Companhia do Metropolitano de São Paulo, exploram questões relativas à LGPD. Dentre elas, que a implementação do sistema de reconhecimento facial não ocorreu conforme à referida lei e que o uso se dá de forma desproporcional e abusiva (BRASIL, 2022). É dispositivo legal, por exemplo, o consentimento dos usuários no tratamento de dados pessoais, conforme art. 5º, inciso XII da LGPD. Entretanto, conforme coleta de provas nos autos do processo em questão, foi demonstrado que a Companhia do Metropolitano de São Paulo falhou em apresentar medidas para coleta de consentimento dos usuários, fato confirmado pela própria ré (BRASIL, 2022), e ainda, há clara violação do direito à privacidade: “tratando-se de um sistema de reconhecimento facial massivo, implementado sobre todos os usuários do metrô, há uma clara incompatibilidade com o direito à privacidade (art. 5º, X, LXXII e LXXIX da CRFB)” (BRASIL, 2022, p. 32).

No mesmo sentido, na Ação Popular contra o edital do projeto “Smart Sampa”, encontra-se menção a violação do art. 23 da Lei Geral de Proteção de Dados. O artigo da lei disciplina que “deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público”. Dessa maneira, uma vez que não há evidências claras da finalidade e interesse público no tratamento de dados pessoais pelas pessoas jurídicas de direito público, “por consequência lógica-jurídica, restam violados os princípios norteadores da proteção de dados, configurando indevida invasão à privacidade, violação da intimidade, honra e imagem, e principalmente, uma violação de direitos humanos” (BRASIL (b), 2023, p. 16). Por conseguinte, a violação dos direitos mencionados é racional adotado para fundamentar a decisão da 3ª Vara de Fazenda Pública que suspendeu o pregão do “Smart Sampa”.

O sistema de reconhecimento facial ainda ameaça gravemente o tratamento de dados pessoais, pois informações podem ser captadas, processadas e armazenadas em ampla escala sem qualquer consulta dos cidadãos cujas imagens são capturadas, e nesse particular há violação de relevantes fundamentos da Lei Geral de Proteção de Dados Pessoais (LGPD), a Lei n. 13.709/2018. A proteção de dados tem por fundamentos legais o respeito à privacidade (art. 2º, I), inviolabilidade da intimidade, honra e imagem (IV), proteção dos direitos humanos e dignidade e exercício da cidadania (VII), conjunto de direitos fortemente em risco pela possibilidade de indicações infundadas da prática de crime geradas por esse sistema de monitoramento, o que resulta em ameaça, novamente, de outros direitos fundamentais, tais como a inviolabilidade da honra e da imagem previstos no art. 5º, X, da Constituição (BRASIL (b), 2023, p. 457).

Conclui-se que, ocorre a violação do direito à proteção de dados pessoais, e em



decorrência disso, a violação do direito à privacidade e do direito de imagem. Sendo que, a violação de apenas um direito pode prejudicar o exercício de outros direitos fundamentais, uma vez que eles estão vinculados e se relacionam, dependendo uns dos outros para sua efetividade na prática.

4. BENEFÍCIOS DO USO DE NOVAS TECNOLOGIAS PARA POLÍTICAS DE SEGURANÇA PÚBLICA

Ainda que a problemática suscitada da violação de direitos fundamentais com a implementação de novas tecnologias exista, é inegável que a inovação tecnológica auxilia na eficácia dos serviços de segurança pública e é imprescindível que o Brasil tem o papel de se aperfeiçoar nesse sentido, a fim de garantir o desenvolvimento nacional. No que se refere ao projeto “Smart Sampa”, uma das justificativas é justamente o uso da tecnologia em prol da sociedade.

Nós acreditamos que esse tipo de tecnologia tem que vir em favor da sociedade. Isso vai melhorar muito o sistema de segurança do Metrô e vai permitir também à Polícia, com o banco de dados de pessoas desaparecidas, fazer essa identificação. Ninguém cria um sistema como esse e investe R\$ 58 milhões para gerar discriminação e fazer mau uso. O objetivo do governo de SP e do Metrô é usar essa tecnologia em favor do cidadão (METRÔ, 2023).

A título de exemplo, no que concerne à eficácia nas medidas de segurança pública, a polícia militar do Estado do Rio de Janeiro realizou mais de trinta prisões em menos de dois meses ao fazer o uso do sistema de reconhecimento facial, onze prisões foram feitas durante o carnaval. Entre os presos, estavam pessoas procuradas pelos crimes de homicídio, feminicídio, associação ao tráfico, furto e roubo à mão armada (FORAGIDO, 2024).

O art. 5º da Constituição Federal prevê que o direito à segurança é um direito fundamental, enquanto o art. 411 do mesmo diploma legal disciplina que a segurança pública é um dever do Estado. Sendo assim, as problemáticas que envolvem o uso de reconhecimento facial não são indicativos para a extinção da tecnologia, ou seja, o conflito entre o direito fundamental de segurança e os demais direitos fundamentais envolvidos não é, por si só, pressuposto para a extinguir o uso de reconhecimento facial.

Em vista disso, acrescenta o autor José Carlos Medeiros de Aragão sobre o conflito de direitos fundamentais “O tema é de complexa resolução – primeiramente, porque não

existe acordo quanto a se existem ou não conflitos entre direitos fundamentais; em seguida, porque estes estão expressos por normas constitucionais e possuem mesma hierarquia e força vinculativa” (ARAGÃO, 2011, p. 9). Portanto, fica esclarecido que apesar de não haver consenso doutrinário sobre o conflito entre direitos fundamentais, resta claro que no caso em questão há o choque entre o direito de segurança pública e os demais direitos fundamentais, conclui-se que na verdade: “possuem a mesma hierarquia e força vinculativa” devendo ambos os direitos coexistirem.

Logo, para garantir de forma concomitante o exercício da inovação tecnológica para fins de segurança pública e a garantia dos direitos fundamentais, é necessário que ocorra prévia regulamentação na implementação dessas tecnologias, visando afastar o conflito entre os direitos fundamentais mencionados e incentivar as iniciativas tecnológicas pelos poderes públicos de forma segura e eficiente.

5. REGULAMENTAÇÃO DE NOVAS TECNOLOGIAS QUE FAZEM O USO DE RECONHECIMENTO FACIAL

Uma das iniciativas de regulamentação de inteligência artificial no Brasil é o Projeto de Lei nº 2338 de 2023, proposto pelo Senador Rodrigo Pacheco (PSD/MG). O objetivo da lei, conforme art. 1º, é “proteger os direitos fundamentais e garantir a implementação de sistemas seguros e confiáveis, em benefício da pessoa humana, do regime democrático e do desenvolvimento científico e tecnológico”.

De modo geral, o Projeto de Lei menciona diversos direitos das pessoas afetadas por sistemas de inteligência artificial, como o direito à informação prévia quando essas pessoas tiverem interação com sistemas de inteligência artificial, direito à explicação sobre decisões feitas por inteligência artificial, bem como o direito de contestação dessas decisões, direito à determinação e à participação humana em decisões feitas por esses sistemas, direito à não-discriminação e correção de vieses discriminatórios e o direito à privacidade.

Prevê, ainda, a categorização dos riscos de sistemas de inteligência artificial, normas de governança a serem tomadas pelos agentes que utilizam essa tecnologia, avaliação de impacto algorítmico, hipóteses de responsabilidade civil, códigos de boas práticas e de governança, comunicação de incidentes graves, supervisão, fiscalização e sanções administrativas.



Com relação à regulamentação de inteligência artificial fora do Brasil, foi aprovado em 2024 o Regulamento de Inteligência Artificial na Europa, que influenciou na elaboração do Projeto de Lei nº 2338 de 2023 em alguns pontos, como a classificação de riscos dos sistemas inteligência artificial, sendo que quanto maior o risco, maior a regulamentação. Nesse sentido, a lei europeia, no mesmo sentido do Projeto de Lei brasileiro, traz que uma das aplicações proibidas é justamente os sistemas de categorização biométrica (reconhecimento facial), sobretudo a identificação biométrica em tempo real.

As imprecisões técnicas dos sistemas de IA destinados à identificação biométrica remota de pessoas singulares podem conduzir a resultados tendenciosos e implicar efeitos discriminatórios. Esses possíveis resultados tendenciosos e efeitos discriminatórios são particularmente relevantes no que diz respeito à idade, etnia, raça, sexo ou deficiências (ARTIFICIAL, 2024).

Por essa razão, a lei menciona que “a utilização para efeitos de aplicação da lei de um sistema de identificação biométrica remota em tempo real em espaços de acesso público estará sujeita a uma autorização prévia concedida por uma autoridade judicial ou por uma autoridade administrativa” (REGULAMENTO, 2024) além disso, os sistemas de IA devem ser supervisionados por pessoas, em vez de serem automatizados, para evitar resultados prejudiciais (LEI, 2024).

5.1. Como o Projeto de Lei nº 2338 de 2023 que regula a Inteligência Artificial no Brasil incidiria no programa “Smart Sampa”

A proposta de regulamentação de inteligência artificial no Brasil traz algumas especificidades normativas que tratam sobre a ferramenta de reconhecimento facial. O art. 7º, 2§ menciona que pessoas expostas a sistemas de reconhecimento de emoções ou a sistemas de categorização biométrica serão informadas sobre a utilização e o funcionamento do sistema no ambiente em que ocorrer a exposição. Ou seja, sendo o sistema de reconhecimento facial uma categorização biométrica, no caso de aprovação do Projeto de Lei nesses termos, a Prefeitura de São Paulo responsável pelo programa “Smart Sampa” deverá diligenciar medidas para que as pessoas que são expostas a esses sistemas sejam informadas, para assegurar que o programa “Smart Sampa” esteja em concordância legal.

Ademais, conforme o Instrumento Particular de 1ª Alteração Contratual Do Compromisso De Consórcio Da Smart City SP, documento extraído do processo judicial que questiona a legitimidade do projeto “Smart Sampa”, consta o rol de responsabilidades técnicas



de uma das empresas contratadas, o qual explica o sistema de reconhecimento facial.

Com o reconhecimento facial, o software é capaz de identificar e comparar rapidamente as faces capturadas pelas câmeras com uma base de dados de procurados ou desaparecidos. Gerencie listas de permissões e bloqueios de forma simples e eficiente. Receba alertas em tempo real quando alguém for detectado com todos os dados e uma rota até o local (BRASIL (b), 2023, p. 451).

Logo, a descrição trata do uso de reconhecimento facial como mecanismo para encontrar pessoas “procuradas ou desaparecidas”. Em vista disso, o Capítulo III, Seção II do Projeto de Lei, veda a utilização de inteligência artificial tida como “risco excessivo” e o art. 15 faz menção importante no que tange à utilização de reconhecimento facial no âmbito das atividades de segurança pública. O artigo disciplina que, será necessária autorização judicial, bem como previsão em lei federal específica para os casos mencionados nos incisos, assim, o programa “Smart Sampa”, no caso da aprovação do Projeto de Lei e nos moldes do art. 15, deverá seguir o disposto na norma.

Art. 15. No âmbito de atividades de segurança pública, somente é permitido o uso de sistemas de identificação biométrica à distância, de forma contínua em espaços acessíveis ao público, quando houver previsão em lei federal específica e autorização judicial em conexão com a atividade de persecução penal individualizada, nos seguintes casos: I – persecução de crimes passíveis de pena máxima de reclusão superior a dois anos; II – busca de vítimas de crimes ou pessoas desaparecidas; ou III – crime em flagrante.

No entanto, ainda que sem regulamentação prévia e com a queda da liminar que suspendeu o andamento do pregão do “Smart Sampa”, em maio de 2023 (MELLO, 2024), o programa teve andamento e em 2024 avançou com 10 mil câmeras em funcionamento. A plataforma de monitoramento localizou uma mulher desaparecida, por meio do banco de dados da Secretaria Municipal de Direitos Humanos e Cidadania (SMDHC) e mais outras quatro pessoas desaparecidas foram localizadas. Também foram realizadas as prisões em flagrante de dois suspeitos que furtavam peças de um veículo estacionado (PROGRAMA, 2024). Sendo assim, o encontro de pessoas desaparecidas e a prisão decorrente de crimes em flagrante são casos que incidem maior regulamentação, já que de acordo com o Projeto de Lei, são aplicações da inteligência artificial consideradas como “risco excessivo”. Além disso, o art. 17 do Projeto de Lei classifica como sistemas de inteligência artificial de alto risco hipóteses que também se aplicariam no programa “Smart Sampa”, como o uso de sistemas biométricos de identificação, investigação criminal e segurança pública, entre outros.

Pensando na mitigação de riscos no uso de sistemas de inteligência artificial, o art. 19,



II do Projeto de Lei estabelece que a estrutura de governança dos agentes de inteligência artificial deverá observar medidas de transparência: “II – transparência quanto às medidas de governança adotadas no desenvolvimento e emprego do sistema de inteligência artificial pela organização”. Além disso, o art. 22 estabelece que a avaliação de impacto algorítmico é obrigação dos agentes de inteligência artificial, no caso de sistemas de alto risco. Será exigido a elaboração de relatórios, que poderão abarcar os possíveis impactos nos direitos fundamentais: “Art. 23 A avaliação de impacto algorítmico será realizada por profissional ou equipe de profissionais com conhecimentos técnicos, científicos e jurídicos necessários para realização do relatório e com independência funcional”.

A Defensoria Pública do Estado de São Paulo apresentou quesitos¹ no processo judicial relacionado ao caso “Smart Sampa” justamente questionando a transparência no emprego da ferramenta de reconhecimento facial, bem como se ocorreu a elaboração de relatórios que abrangem outros direitos, além daqueles referentes à proteção de dados pessoais.

Cumpre ainda destacar que, em linha com o art. 9 do Projeto de Lei, pessoas afetadas por decisões feitas por sistemas de inteligência artificial têm o direito de contestar essas decisões que produzam efeitos jurídicos relevantes. A título de exemplo, a pessoa que teve sua prisão decretada em decorrência de uma decisão feita por um sistema de reconhecimento facial terá o direito de contestar essa decisão dentro do processo penal, não obstante, ainda que não haja a aprovação do Projeto de Lei, o direito de contestar já é mera garantia processual de ampla defesa e contraditório.

Assim sendo, a forma como se dará essa contestação, especialmente em um processo penal, ainda é uma incógnita, uma vez que, para garantir uma boa defesa do acusado, é necessária perícia técnica especializada para comprovar se a decisão feita pela inteligência artificial foi errônea ou partiu de um viés discriminatório. Entretanto, em razão de essa ser uma nova tecnologia, a demanda por profissionais do direito que entendem desses aspectos será ainda mais alta, e o direito de contestar as decisões feitas por um sistema de inteligência

¹ Os quesitos foram apresentados à perícia a ser realizada na Ação Popular nº 1027876-45.2023.8.26.0053 em 01 de fevereiro de 2024 e até 11 de agosto de 2024, aguarda-se a resposta desses quesitos. Os principais quesitos sobre transparência e elaboração de relatório foram: “3. A Prefeitura divulgou de forma adequada quais dados serão coletados e tratados, de quantas pessoas, com quem serão compartilhados, a quais outras bases de dados ele terá acesso para fazer as comparações inerentes à funcionalidade da tecnologia? a. Ainda, divulgou os custos envolvidos, os riscos presentes e as medidas tomadas para prevenção e mitigação desses riscos?” e “7. Para além da realização de um Relatório de Impacto à Proteção de Dados/RIPD, houve a realização de um relatório de impacto a direitos que seja mais abrangente do que a proteção a dados pessoais em específico?”.



artificial é questionável diante de tantas inseguranças trazidas pelo uso da ferramenta.

Dada a opacidade da análise algorítmica e da tomada de decisão, em particular ao empregar métodos de inteligência artificial, os resultados discriminatórios do perfilamento algorítmico podem muitas vezes ser menos óbvios e mais difíceis de detectar do que as decisões humanas e, portanto, mais difíceis de contestar. Além da opacidade da IA, defensores dos direitos humanos em todo o mundo não estão tecnologicamente equipados para identificar essas práticas discriminatórias (COMITÊ, 2024, p. 11-12).

6. CONSIDERAÇÕES FINAIS

Apesar das controvérsias jurídicas acerca do caso “Smart Sampa”, a decisão do Agravo de Instrumento que possibilitou o andamento do projeto “Smart Sampa”, proferida pela 3ª Câmara de Direito Público do Tribunal de Justiça de São Paulo em 23 de maio de 2023, concluiu que “não há evidência de que a implementação de videomonitoramento reforce eventual discriminação social e racial” (BRASIL (a), 2023, p. 496), também mencionou que a Lei Geral de Proteção de Dados não se aplica para os fins exclusivos de segurança pública.

De acordo com o art. 4º, III, “a” e “d”, a LGPD não se aplica ao tratamento de dados pessoais realizado para fins exclusivos de segurança pública e atividades de investigação e repressão de infrações penais, de maneira que, ao menos em cognição sumária, não se verifica qualquer ilegalidade nos termos do edital (BRASIL (a), 2023, p. 496).

Contudo, ainda que a decisão judicial fundamente sobre a inaplicabilidade da LGPD para fins exclusivos de segurança pública, cumpre destacar que a regulamentação de inteligência artificial na Europa demonstra para o mundo que o uso dessas tecnologias depende de regulamentação específica. O mero amparo em legislações auxiliares, como a própria LGPD, não é suficiente, especialmente se tratando de uma tecnologia de implementação em massa, fato que demanda maior respaldo jurídico. Logo, a instalação de um programa como este, sem prévia regulamentação, está em contramão ao que os países desenvolvidos têm feito, ainda que nada impeça que os protocolos adotados pelos poderes públicos no Brasil observem os aspectos de regulamentação internacional.

Entretanto, apesar das discussões judiciais relacionadas ao uso de sistemas de reconhecimento facial em espaços públicos, em 04 de julho de 2024, a Prefeitura de São Paulo inaugurou a Central de Monitoramento do “Smart Sampa”, o prefeito de São Paulo, Ricardo Nunes, comenta: “não vamos medir esforços para tornar a cidade cada dia mais segura com o aumento do efetivo agora somado ao uso da tecnologia. Foi isso que a gente estudou em todas as grandes cidades do mundo que melhoraram seus índices de segurança”

(PREFEITURA, 2024), dessa forma, o programa “Smart Sampa” segue em funcionamento.

É necessário voltar alguns passos, especialmente pela garantia de direitos fundamentais, que é requisito superior para direcionar os atos dos poderes públicos. Significa que a regulamentação prévia da implementação dessas tecnologias é crucial para fazer valer os direitos fundamentais do homem. O amparo em leis auxiliares ou a iniciativa dos poderes públicos em incentivar medidas de inovação tecnológica não podem se sobrepor à garantia de direitos fundamentais, sendo assim, a doutrina reitera: “os atos dos poderes constituídos devem conformidade aos direitos fundamentais e se expõem à invalidade se os desprezarem” (MENDES; BRANCO, 2012, p. 218).

Sendo assim, cumpre retomar que o programa “Smart Sampa” tem sido alvo de discussões judiciais², devido as possíveis violações de direitos fundamentais. Foram identificados potenciais infrações a direitos constitucionais, tais como liberdade, presunção de inocência e privacidade. Ainda, constatou-se que, caso seja aprovado o Projeto de Lei que visa regulamentar a inteligência artificial no Brasil, o programa “Smart Sampa” estaria em desacordo com disposições propostas por tal projeto. Essas problemáticas demonstram que a iniciativa da Prefeitura de São Paulo está gerando controvérsias jurídicas que poderão ser mais amplamente discutidas no futuro.

Por fim, para assegurar a coexistência do direito à segurança, especialmente no que se refere à segurança pública, com outros direitos fundamentais, é imprescindível que haja uma regulamentação prévia por meio de legislação específica para sistemas de reconhecimento facial. Embora o programa “Smart Sampa” esteja implementado sem uma regulamentação específica, é evidente que os benefícios proporcionados pela tecnologia de inteligência artificial, que utiliza o reconhecimento facial para fins de segurança pública, não compensam os potenciais danos advindos de possíveis violações aos direitos fundamentais.

7. REFERÊNCIAS

ABELLO, Antonio A; ARAÚJO, Rafael Will M. de; HIRATA JR, R. Parecer InternetLab. **InternetLab**, [s.l.]. Disponível em: <<https://internetlab.org.br/wp-content/uploads/2022/03/Parecer-Metro-de-Sao-Paulo.-Reconhecimento-facial.pdf>>. Acesso em: 29 jul. 2023.

² Em 13 de agosto de 2024, a Ação Popular nº 1027876-45.2023.8.26.0053 que discute a legitimidade do programa “Smart Sampa” aguarda desfecho do Agravo de Instrumento interposto pela Prefeitura do Município de São Paulo.



ARAGÃO, J. C. M. de. **Choque entre direitos fundamentais Consenso ou controvérsia?** Revista de Informação Legislativa. Brasília a. 48 n. 189 jan./mar. 2011.

ARTIFICIAL Intelligence Act. **PARLAMENTO EUROPEU**, [s.l.]. Disponível em: <https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.html#title2>. Acesso em: 29 jul. 2024.

BRASIL (a). **Tribunal de Justiça do Estado de São Paulo** (3ª Câmara de Direito Público), Agravo de Instrumento nº 2122169-52.2023.8.26.0000. Agravante: Município de São Paulo: Agravado: Silvia Andrea Ferraro. Relatora Paola Lorena. São Paulo, 23 maio 2023.

BRASIL (b). **Tribunal de Justiça do Estado de São Paulo** (3ª Vara da Fazenda Pública), Ação Popular nº 1027876-45.2023.8.26.0053. Requerente: Silvia Andrea Ferraro e outros. Requerido: Prefeitura Municipal de São Paulo e outros. Juiz de Direito Dr. Luiz Manuel Fonseca Pires. São Paulo, 18 maio 2023.

BRASIL. **Tribunal de Justiça do Estado de São Paulo** (6ª Vara de Fazenda Pública). Ação Civil Pública nº 1010667-97.2022.8.26.0053. Requerente: Defensoria Pública do Estado de São Paulo e outros. Requerido: Companhia do Metropolitano de São Paulo. Juíza de Direito Dra. Cynthia Thomé. São Paulo, 22 mar. 2022.

COMITÊ para a Eliminação da Discriminação Racial. **ACNUDH**, [s.l.]. Disponível em: <https://acnudh.org/wp-content/uploads/2020/12/CERD_C_GC_36_PORT_REV.pdf>. Acesso em: 29 jul. 2024.

FORAGIDO há 17 anos, homem é preso por reconhecimento facial no centro do Rio. **G1**, [s.l.]. Disponível em: <<https://g1.globo.com/rj/rio-de-janeiro/noticia/2024/02/26/homem-e-preso-por-reconhecimento-facial-no-centro-do-rio.ghtml>>. Acesso em: 24 jul. 2024.

IBGE. **Desigualdades sociais por cor ou raça no Brasil**. Rio de Janeiro: IBGE, 2019. 12 p. (Complemento 2; v. 41).

LEI da UE sobre ia: primeira regulamentação de inteligência artificial. **Parlamento Europeu**, [s.l.]. Disponível em: <<https://www.europarl.europa.eu/topics/pt/article/20230601STO93804/lei-da-ue-sobre-ia-primeira-regulamentacao-de-inteligencia-artificial>>. Acesso em: 24 jul. 2024.

MELLO, Daniel. Justiça libera edital de câmeras com reconhecimento facial em SP. **Agência Brasil**, São Paulo. Disponível em: <<https://agenciabrasil.ebc.com.br/justica/noticia/2023-05/justica-libera-edital-de-cameras-com-reconhecimento-facial-em-sp>>. Acesso em: 24 jul. 2024.

MENDES, G.F.; BRANCO, P.G.G. **Curso de Direito Constitucional**. São Paulo: Saraiva, 2012.

METRÔ de SP inicia operação de sistema de reconhecimento facial; TJ chegou a impedir instalação. **G1**, São Paulo. Disponível em: <<https://g1.globo.com/sp/sao-paulo/noticia/2022/11/21/metro-de-sp-inicia-operacao-de-novo-sistema-de-monitoramento-eletronico-por-meio-de-reconhecimento-facial-tj-chegou-a-impedir-instalacao.ghtml>>. Acesso em: 24 jul. 2023.

OLIVEIRA S. **Inteligência Artificial, Proteção de Dados Pessoais e Responsabilidade na Era Digital**. São Paulo, Thomson Reuters Brasil, 2021.

PREFEITURA inaugura central de monitoramento do smart sampa com câmeras inteligentes em operação 24h. **Prefeitura de São Paulo**, São Paulo. Disponível em: <<https://capital.sp.gov.br/w/prefeitura-inaugura-central-de-monitoramento-do-smart-sampa-com-c%C3%A2meras-inteligentes-em-opera%C3%A7%C3%A3o-24h>>. Acesso em: 24 jul. 2024.

PROGRAMA smart sampa avança na capital com 10 mil câmeras em funcionamento. **Prefeitura de São Paulo**, São Paulo. Disponível em: <https://www.prefeitura.sp.gov.br/cidade/secretarias/seguranca_urbana/noticias/index.php?p=365363>. Acesso em: 24 jul. 2024.

REGULAMENTO de Inteligência Artificial: Parlamento aprova legislação histórica. **EUROPARLAMENTO**, [s.l.]. Disponível em: <<https://www.europarl.europa.eu/news/pt/press-room/20240308IPR19015/regulamento-inteligencia-artificial-parlamento-aprova-legislacao-historica>>. Acesso em: 12 ago. 2024.

SARLET, I. W. **A Eficácia dos Direitos Fundamentais**. São Paulo: Livraria do Advogado, 2009.

SARLET, I. W.; MARINONI, L.G.; MITIDIERO, D. **Curso de Direito Constitucional**. São Paulo: Saraiva, 2017.

SARLET; Ingo. A EC 115/22 e a proteção de dados pessoais como Direito Fundamental I. **Conjur**, [s.l.]. Disponível em: <<https://www.conjur.com.br/2022-mar-11/direitos-fundamentais-ec-11522-protacao-dados-pessoais-direito-fundamental/>>. Acesso em: 16 ago. 2024.

SILVA, J. A. da. **Curso de Direito Constitucional Positivo**. São Paulo: Malheiros Editores, 2017.

SISTEMA de reconhecimento facial enviou este homem inocente para a prisão. **CNN BRASIL**, [s.l.]. Disponível em: <<https://www.cnnbrasil.com.br/internacional/sistema-de-reconhecimento-facial-enviou-este-homem-inocente-para-a-prisao/>>. Acesso em: 29 jul. 2024.

TEIXEIRA, Raoni F. da S.; JANUZI, Rafael B.; FARIA, Fabio A. The Brazilian Data at Risk in the Age of AI?. In: **Encontro nacional de inteligência artificial e computacional (ENIAC)**, 19. 2022, Campinas/SP. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2022. p. 413-424. ISSN 2763-9061. Disponível em: <<https://doi.org/10.5753/eniac.2022.227520>>. Acesso em: 07 abr. 2023.

VIDEOMONITORAMENTO: Webreport. **INSTITUTO IGARAPÉ**, [s.l.]. Disponível em: <<https://igarape.org.br/videomonitoramento-webreport/>>. Acesso em: 29 jul. 2024.

Contatos: giovanna_albuquerque26@hotmail.com e eduardoariente@gmail.com.