DIGA NÃO AO SMART SAMPA

TIRE MEU ROSTO DA SUA MIRA

DIGA NÃO AO SMART SAMPA

TIRE MEU ROSTO DA SUA MIRA

SUMÁRIO

INTRODUÇÃO - O QUE É SMART SAMPA?.....4

1. PROTEÇÃO DE DADOS E PRIVACIDADE AMEAÇADAS.....5

2. RISCOS DE SEGURANÇA.....6

3. PROBLEMAS NA POLÍTICA URBANA.....7

4. CUSTOS, (IN)EFICÁCIA E DESIGUALDADE.....9

CONCLUSÃO.....12

INTRODUÇÃO - O QUE É SMART SAMPA?

No dia 17 de novembro de 2022, a Prefeitura do Município de São Paulo, pela Secretaria Municipal de Segurança Urbana, tornou público que realizaria licitação na modalidade pregão eletrônico, edital n. 079/SMSU/2022 da Secretaria Municipal de Segurança Urbana de São Paulo, com critério de julgamento de menor preço, objetivando a *"contratação de serviço de videomonitoramento, com o fornecimento de toda a estrutura de equipamentos e mão-de-obra necessária para disponibilização, tratamento e armazenamento das imagens a serem capturadas"*. O edital também teve como objetivo a contratação de estrutura técnica e de gestão para uma plataforma de automação de vigilância e monitoramento, que prevê a integração e interoperabilidade de vários sistemas de coleta e processamento de informações sobre pessoas, veículos, perímetros territoriais e detecção de movimentos e fluxos.

O uso de tecnologias como as de reconhecimento facial nos espaços públicos leva a um processo de vigilância em massa da população, que - para além dos danos decorrentes de processos discriminatórios recorrentemente observados - pode inibir o exercício da liberdade de expressão em situações como de manifestações nos espaços das cidades.

Ressalta-se que o Edital Smart Sampa prevê o monitoramento de eventos como manifestações e greves também por mídias sociais, o que torna o endereçamento ainda mais precário. Trata-se, então, de cenário capaz de afetar negativamente uma série de direitos fundamentais e sua fruição individual e coletiva no espaço urbano.

O "Smart Sampa" promete trazer modernidade e conveniência para nossas vidas, no entanto, os impactos negativos são muitos e **irreversíveis**. Há muito em jogo: privacidade, proteção de dados pessoais, segurança, reformulações na prestação

de serviços públicos, danos irreparáveis em decorrência das escolhas implicadas neste projeto. É hora de nos unirmos e dizermos não a um projeto tão perigoso!

1. PROTEÇÃO DE DADOS E PRIVACIDADE AMEAÇADAS

A implementação do Smart Sampa significa que nossos movimentos e atividades cotidianas serão monitorados constantemente, sob o risco de uma vigilância massiva.

Há um altíssimo risco do uso da tecnologia para perseguição de manifestantes, além de perfilamento racial. Primeiramente, durante as manifestações do movimento Black Lives Matter nos Estados Unidos, que pediam por justiça após o assassinato de George Floyd, as tecnologias de reconhecimento facial foram utilizadas para registrar dados biométrico dos manifestantes e - dessa forma - persegui-los.

Não só nos Estados Unidos, como também na China, o governo teria utilizado reconhecimento facial aliado à integração com outros serviços de vigilância para fazer perfilamento racial de pessoas Uighurs.

Considerando que a proteção dados pessoais é um direito fundamental, recentemente consagrado na constituição federal, em seu art. 5º, inciso LXXIX, as câmeras de reconhecimento facial violarão todos os dias os direitos de cidadãs e cidadãos que estiverem circulando na cidade de São Paulo, porque seus dados biométricos estariam sendo coletados sem seu consentimento. Além disso, há o perigo desses dados serem indevidamente utilizados por empresas parceiras.

A LGPD não se aplica aos dados tratados na questão de segurança pública. Ainda não tem nenhuma lei regulamentando e/ou regulando o uso de dados pessoais no âmbito da segurança pública. Dessa forma, a implementação do Smart Sampa

fere diretamente direitos fundamentais de todas as pessoas que transitam e transitarão pela cidade de São Paulo.

→ **Intercept Brasil**
A Bahia está virando um laboratório de reconhecimento facial

Nossos dados pessoais serão coletados, armazenados e possivelmente compartilhados com terceiros, sem nosso consentimento. Diga não ao vigilantismo em massa das pessoas!

→ **ZAP Notícias**
Black Lives Matter. Agências federais usaram reconhecimento facial durante manifestações

→ **Vice**
Six Federal Agencies Used Facial Recognition On George Floyd Protestors

2. RISCOS DE SEGURANÇA

O edital do Smart Sampa, prevê a interoperabilidade de sistemas e dados, ou seja, haverá uma integração entre secretarias. A crescente conectividade do *Smart Sampa*, aumenta também os riscos de segurança. Hackers e criminosos cibernéticos podem explorar vulnerabilidades do sistema para acessar suas informações pessoais ou até mesmo controlar dispositivos domésticos inteligentes. Proteja-se dizendo não aos riscos de segurança do Smart Sampa!

Todos os dias todas as pessoas que transitam em São Paulo serão monitoradas 24h por dia. Os riscos são altíssimos. Recentemente o PCC (Primeiro Comando da Capital) - Facção Criminosa, fez uso de câmeras da cidade de São Paulo para monitorar viaturas da polícia civil. Se facções criminosas podem hackear o sistema e usar para monitorar a Polícia, imaginem o que pode ser feito com cidadãos anônimos?

→ **Uol Notícias**
PCC acessou câmeras do Governo de SP para monitorar viatura da Polícia Civil

3. PROBLEMAS NA POLÍTICA URBANA

O edital do Smart Sampa não previu uma análise de impacto a direitos prévia à licitação, especialmente quanto às câmeras de reconhecimento facial que foram mencionadas no edital, principalmente na população mais vulnerabilizada.

O uso de tecnologias como as de reconhecimento facial nos espaços públicos leva a um processo de vigilância em massa da população, que - para além dos danos decorrentes de processos discriminatórios recorrentemente observados - pode inibir o exercício da liberdade de expressão em situações como de manifestações nos espaços das cidades. Cidades como São Francisco, na Califórnia, que antes tinham implementado o uso de reconhecimento facial na política de segurança pública, voltaram atrás e baniram o uso, tendo em vista os riscos aos direitos fundamentais de seus cidadãos e o risco grave ao psicológico de seus cidadãos, uma vez que a sensação de estar sendo vigiado o tempo inteiro é brutal.

A população mais vulnerabilizada já sofre os estigmas de uma sociedade, ou seja, um tipo de etiquetamento. Pessoas que estão em situação de rua sofrem estigmas brutais, além do sofrimento ocasionado pela falta de uma residência. Assim, as tecnologias de reconhecimento facial reforçam a vulnerabilização daqueles que já são vulneráveis. No edital do *Smart Sampa* as *smart cameras* têm a possibilidade de indicar que pessoas estão em "movimentos suspeitos". Mas **como essas câmeras foram treinadas para reconhecer pessoas em atividades suspeitas?**

As câmeras inteligentes são treinadas para reconhecer pessoas em atividades suspeitas usando um processo chamado aprendizado de máquina. O aprendizado de máquina é um tipo de inteligência artificial que permite que os computadores

aprendam sem serem explicitamente programados. No caso de câmeras inteligentes, o aprendizado de máquina é usado para treinar as câmeras a identificar padrões de comportamento humano associados a atividades suspeitas.

Os dados de treinamento para câmeras inteligentes geralmente são coletados de várias fontes, como imagens de segurança, postagens de mídia social e artigos de notícias. Os dados são usados para treinar um algoritmo de aprendizado de máquina para identificar os padrões associados a atividades suspeitas. Depois que o algoritmo é treinado, ele pode ser usado para analisar novas imagens para identificar pessoas envolvidas em atividades suspeitas.

Existem vários algoritmos de aprendizado de máquina diferentes que podem ser usados para treinar câmeras inteligentes. Alguns dos algoritmos mais comuns incluem máquinas de vetores de suporte, árvores de decisão e redes neurais. A escolha do algoritmo dependerá das características específicas dos dados que estão sendo usados para treinar a câmera.

A precisão das câmeras inteligentes depende de vários fatores, incluindo a qualidade dos dados de treinamento, a complexidade do algoritmo e o ambiente em que a câmera está sendo usada. Em geral, as câmeras inteligentes são mais precisas na detecção de atividades suspeitas[1] em ambientes controlados, como aeroportos e estações de trem. **No entanto, eles são menos precisos na detecção de atividades suspeitas em ambientes não controlados, como as ruas da cidade.**

As câmeras inteligentes têm o potencial de ser uma ferramenta valiosa para as agências de segurança e aplicação da lei. No entanto, é importante estar ciente das preocupações de privacidade associadas ao uso de câmeras inteligentes. As câmeras inteligentes podem coletar uma grande quantidade de dados sobre

1. Ramos, Silvia Elemento suspeito [livro eletrônico]: racismo e abordagem policial no Rio de Janeiro / Silvia Ramos...[et al.]; ilustração Miguel Morgado. - Rio de Janeiro : CESeC, 2021.

os movimentos e atividades das pessoas. Esses dados podem ser usados para rastrear os movimentos das pessoas, monitorar seu comportamento e até mesmo identificar suas opiniões políticas. Isso poderia ter um efeito inibidor sobre a liberdade de expressão e as liberdades civis. É importante pesar os potenciais benefícios das câmeras inteligentes em relação às possíveis preocupações com a privacidade antes de implantá-las.

Ressalta-se que o Edital Smart Sampa prevê o monitoramento de eventos como manifestações e greves também por mídias sociais, o que reforça seu caráter nefasto. Trata-se, então, de cenário capaz de afetar negativamente uma série de direitos fundamentais e sua fruição individual e coletiva no espaço urbano.

→ O Panóptico
E quando os dados do seu rosto são coletados sem sua permissão? Conheça a maquiagem anti-vigilância – uma ferramenta de resistência ao reconhecimento facial

→ NY Times
San Francisco Bans Facial Recognition Technology

4. CUSTOS, (IN)EFICÁCIA E DESIGUALDADE

A implementação do Smart Sampa exigirá um alto investimento financeiro, que não corresponde à ausência de cautela na formulação do edital licitado. O custo estimado de implementação do Smart Sampa gira em torno **de 70 milhões anuais até 2028, totalizando R$ 350.000.000,00 (trezentos e cinquenta milhões de reais)** . Ou seja, estamos falando de dispêndio de enormes somas de dinheiro público sem o devido detalhamento da decisão administrativa que deu origem a esse projeto!

A vida de pessoas negras, principalmente de mulheres negras, pessoas não-binárias e pessoas transgênero estará ameaçada a todo momento, tendo em vista que

as tecnologias de reconhecimento facial **erram em mais de 90% com pessoas negras e em 100% com pessoas trans**[2].

Na esteira das desigualdades, o uso de reconhecimento facial pelo Estado de Israel contra o povo palestino[3]. O sistema Blue Wolf, adquirido pelo estado israelense, que através de câmeras e smartphones que captura fotos de rostos de palestinos, que são vinculadas a um banco de dados de imagens. O aplicativo do telefone traz notificações em cores diferentes para alertar os soldados se uma pessoa deve ser detida, se já foi presa ou se não apresenta ameaça. Para construir o banco de dados usado pela Blue Wolf, soldados israelenses fotografaram vários palestinos no ano passado, incluindo crianças e idosos. Além do Blue Wolf, os militares israelenses instalaram câmeras de varredura facial na cidade de Hebron, no sul da Cisjordânia, para ajudar os soldados nos postos de controle a identificar os palestinos antes mesmo de apresentarem suas carteiras de identidade. Uma rede mais ampla de câmeras de circuito fechado de televisão, apelidada de "Hebron Smart City", fornece monitoramento em tempo real da população da cidade.

Implementar uma tecnologia que impactará os cofres da prefeitura e que não se comprova eficaz, além de gerar processos indenizatórios contra a prefeitura, a qual, provavelmente terá que arcar com indenizações por prisões ilegais, armazenamento de dados sem o consentimento dos titulares, uso indevido da tecnologia por pessoas sem treinamento, riscos de *hackers* utilizarem de uma instabilidade no sistema para monitoramento de pessoas. O melhor caminho é a suspensão definitiva do Programa Smart Sampa!

Ao contrário do que se possa pensar, o reconhecimento facial não é uma solução para o problema de identificação de suspeitos por humanos[4], pois a máquina erra

2. Além do racismo, reconhecimento facial erra mais em pessoas trans - 14/02/2021 - UOL TILT

3. Israel vigia palestinos com sistema de reconhecimento facial na Cisjordânia

4. Reconhecimento de pessoas: um campo fértil para o erro judicial

(e com frequência) e, o erro pode levar ao cerceamento ilegal da liberdade, com uma prisão indevida.

No Rio de Janeiro, durante uma operação policial no Estádio do Maracanã em 2019, dos 11 casos de pessoas detidas a partir do uso da tecnologia, sete foram identificados erroneamente pela máquina (63% dos casos)[5].

Em 2021, um pedreiro residente no Piauí foi confundido com um fraudador de cartões de crédito do Distrito Federal e sofreu uma abordagem policial truculenta em sua residência[6], sendo conduzido pela polícia a outro estado sem explicações. O homem ficou preso por três dias até a polícia admitir o erro. Este problema não é exclusivo do Brasil: em Detroit, Estados Unidos, o chefe da polícia local afirmou que o sistema de reconhecimento facial DataWorks Plus, que custou US$ 1 milhão à cidade, tinha uma taxa de erro de cerca de 96%.[7]

Pesquisas têm mostrado que esses sistemas falham mais com mulheres, especialmente mulheres negras[8]. E, por questões técnicas de desenvolvimento, os algoritmos de reconhecimento facial também promovem a exclusão de pessoas transgênero e não-binárias. Além disso, há um padrão comum nos casos de engano ou falha na precisão dos sistemas noticiados no Brasil: a maioria envolve pessoas pretas e pardas. Aliás, mais de 90% das pessoas presas pelo reconhecimento facial são negras.[9]

---

5. UM RIO DE CÂMERAS COM OLHOS SELETIVOS: USO DO RECONHECIMENTO FACIAL PELA POLÍCIA FLUMINENSE
6. 'Disseram que eu era traficante', diz pedreiro preso injustamente - Notícias - R7 Brasília
7. Detroit Police Chief: Facial Recognition Software Misidentifies 96% of the Time
8. http://gendershades.org/overview.html
9. Artigo: Levantamento revela que 90,5% dos presos por monitoramento facial no Brasil são negros

CONCLUSÃO

O futuro de nossa cidade precisa estar em nossas mãos. Esse projeto não representa uma iniciativa dialogada com a população! Diga não ao "Smart Sampa". Lutemos por uma cidade onde a tecnologia seja utilizada de forma responsável e benéfica, sem comprometer nossos direitos fundamentais. Junte-se a nós nessa campanha e diga não ao Smart Sampa!