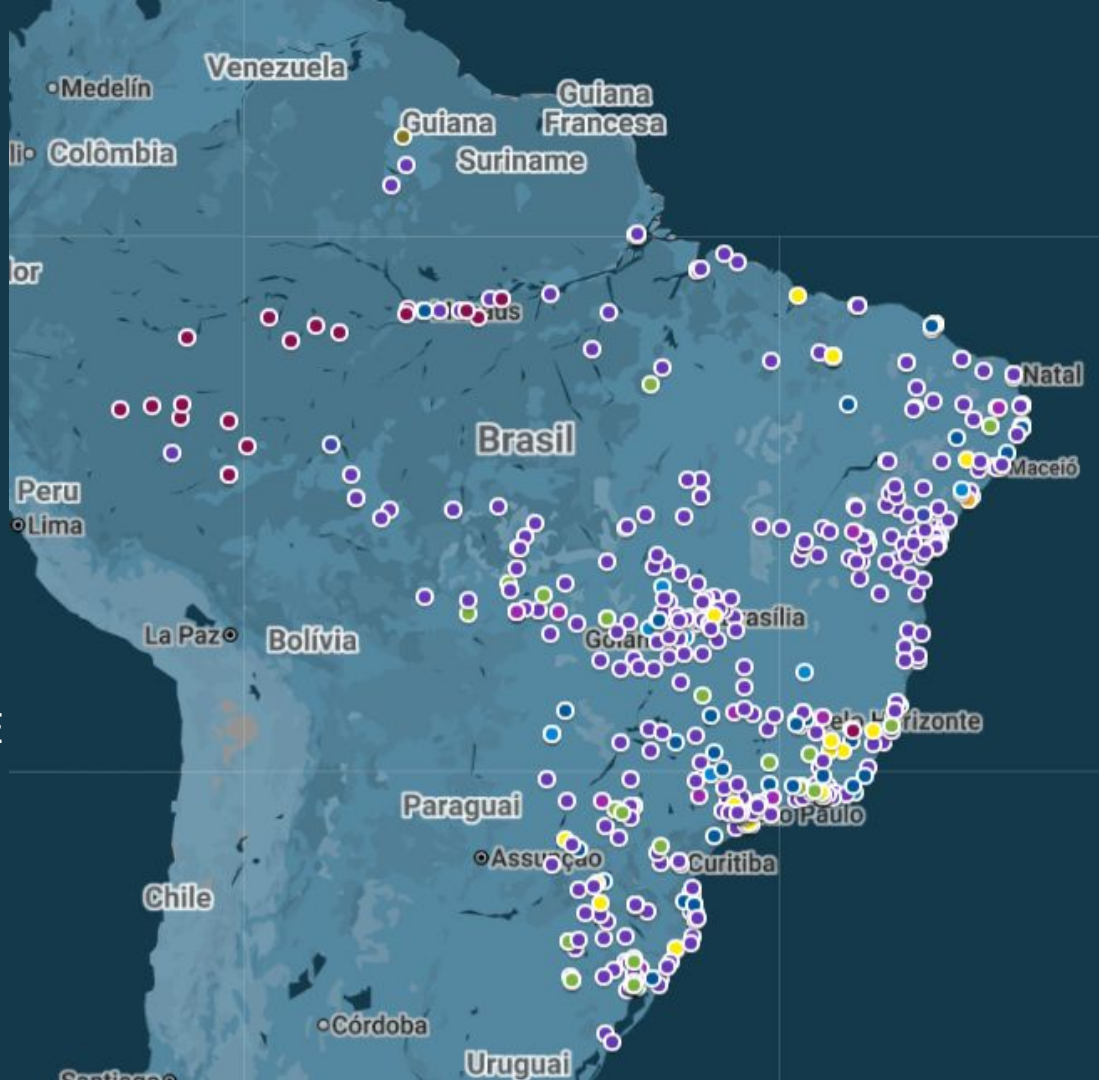
Sistemas de IA no serviço público e em infraestruturas críticas

Pablo Nunes (Coordenador do CESeC)

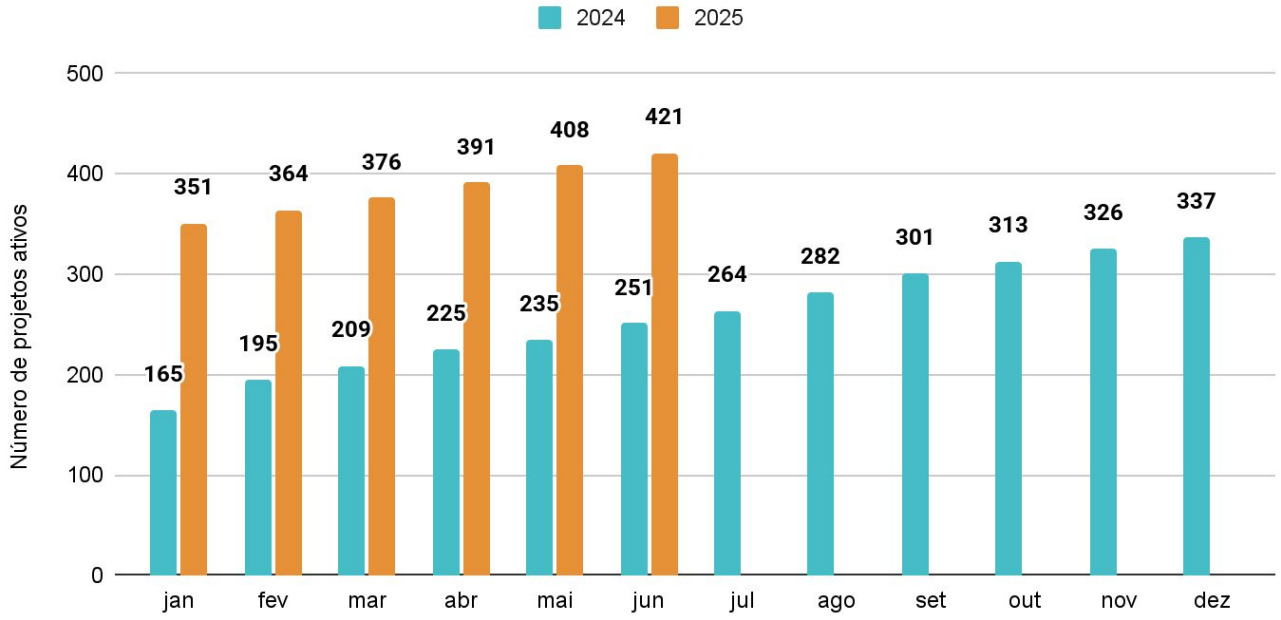
Expansão do reconhecimento facial no Brasil

442 PROJETOS QUE UTILIZAM TÉCNICAS DE RECONHECIMENTO FACIAL NO PAÍS.

87 MILHÕES DE PESSOAS POTENCIALMENTE VIGIADAS POR RECONHECIMENTO FACIAL



Número de projetos de reconhecimento facial registrados por mês (2024 - 2025)



Fonte: O Panóptico | CESeC

Riscos potenciais do uso de TRF na Segurança Pública

- **Vieses discriminatórios**: maior probabilidade de erros contra pessoas negras e periféricas, reforçando desigualdades raciais. Estudos de 2025 demonstram que os vieses permanecem mesmo com o avanço tecnológico.
- **Invasão de privacidade**: coleta massiva de dados biométricos sem consentimento nem transparência.
- **Impacto negativo no policiamento**: gera falsas suspeitas, sobrecarrega a polícia e não contribui para prevenção do crime.
- **Violação do direito à reunião e manifestação:** risco de identificar e intimidar manifestantes e opositores políticos.
- **Restrição ao direito de circulação:** uso em transportes e espaços públicos pode impedir acesso de forma arbitrária.
- **Risco de vazamento de dados sensíveis**: bancos de dados biométricos são alvos de ataques e podem ser usados por atores maliciosos.
- **Dependência tecnológica de fornecedores privados:** fortalece empresas estrangeiras sem controle público, criando riscos de soberania digital.

Estudos de caso de aplicação de TRF na Segurança Pública

Em muitos municípios de Goiás e da Bahia, por exemplo, que receberam verbas para TRF, há falta de internet de alta qualidade, urbanização, saneamento básico, educação e saúde.

O investimento em TRF em GO ocorreu em cidades onde entre **20% e 50% dos alunos da rede pública não têm acesso à internet.**

No caso da Bahia, alguns dos municípios que receberam a tecnologia não tinham cobertura aceitável de saneamento básico. Em alguma cidades, **menos de 5% dos domicílios** eram cobertos pelo serviço de saneamento.

Smart Sampa: vigia, mas não protege

Estudo usou método usado pelo Banco Mundial para avaliar o efeito de políticas públicas (Diff-in-Diff) e mostrou que não houve mudança significativa nos indicadores de criminalidade na cidade de São Paulo com o uso das câmeras de reconhecimento facial. O custo do Smart Sampa é de R$10 milhões por mês.

Figura 1: Furtos (taxa por 100.000 habitantes)

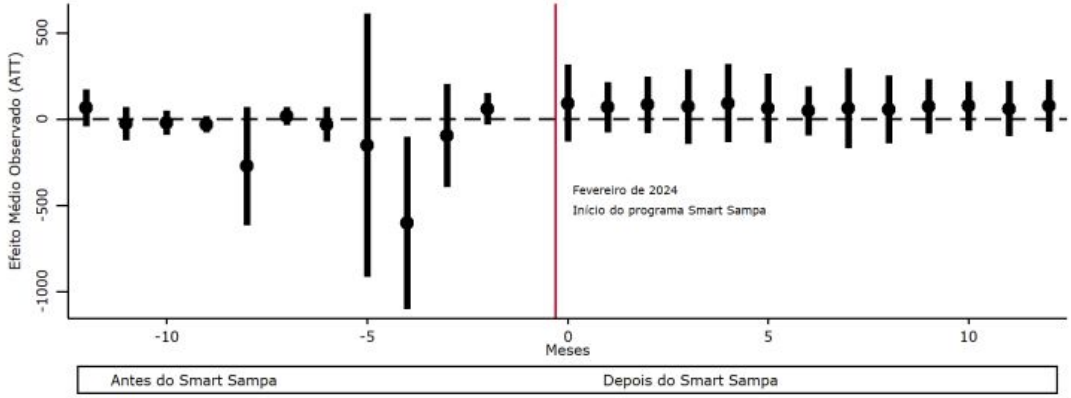
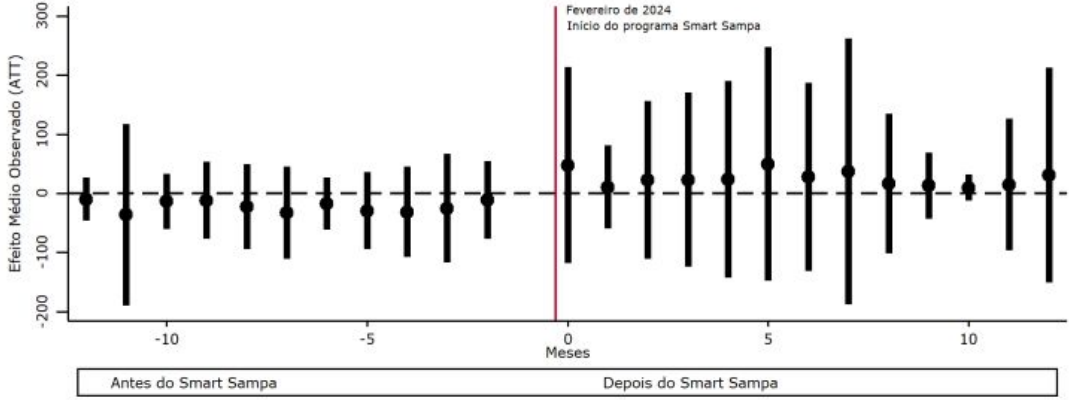


Figura 2: Assaltos (taxa por 100.000 habitantes)



Soberania e infraestruturas críticas

- Delegar dados de cidadãos a empresas, sem governança, **fragiliza infraestruturas críticas.**
- Quem **controla os dados**, controla também as **infraestruturas**.
- Big Techs já oferecem soluções no Brasil; no Judiciário, o ChatGPT é usado em peças processuais, com armazenamento de textos e prompts pela OpenAI.
- Dados seguem regras e interesses estrangeiros, não nacionais, comprometendo **soberania** e **democracia**.
- Algoritmos de **reconhecimento facial** são **vulneráveis** a ataques adversariais (manipulação de imagens e vídeos).
- Vazamentos de dados em infraestruturas críticas atingem tanto a **segurança pública** quanto a **nacional**.
- Garantir soberania passa por **autonomia na gestão de dados** e independência frente às Big Techs.

Discussão das TRF no PL 2338

- O PL classifica como **“risco excessivo”:**

  Art. 13. É proibido o uso de sistemas de IA nos seguintes casos:

  IV – sistemas de identificação biométrica remota em tempo real em espaços de acesso público, exceto quando utilizados:
  a) pelos órgãos de segurança pública, de forma excepcional, quando estritamente necessário para prevenir ameaça concreta ou localizar pessoa específica suspeita de crime grave ou vítima de crime;
  b) para localização de pessoas desaparecidas, nos termos de regulamentação.

- Problemas com essas **exceções**:

  a) **Termos vagos** como “estritamente necessário” e “crime grave” sem definição clara.
  b) Não exige **lei específica** para regulamentar o uso.
  c) Abre margem para **usos abusivos e massivos** sob justificativa de segurança.

Resultado: risco de legitimar TRFs sem garantias mínimas de proteção de dados e direitos fundamentais; estudo de impacto prévio; supervisão independente e transparência. **OU SEJA**, as exceções criam um “**limbo**” regulatório sem governança.

Reivindicações legislativas

Para garantir uma regulação que esteja à altura dos desafios impostos pelas TRFs, propomos:

- **Rever a exceção prevista no artigo 13, inciso IV, que autoriza o uso de TRFs, ainda que sejam reconhecidas como de "risco excessivo". Dada a gravidade dos impactos associados ao seu uso, o caminho mais responsável é sua proibição geral;**
- Submeter as TRFs às mesmas exigências dos sistemas de **"alto risco"**, incluindo **avaliação de impacto** contínua, **auditoria independente**, **supervisão humana** e **mecanismos de contestação;**
- Reescrever o inciso IV para que qualquer uso excepcional dessas tecnologias fique condicionado à **aprovação de legislação específica**, com **salvaguardas robustas** e **cumprimento integral** das obrigações do art. 14, incisos IX a XI;
- Garantir **controle multissetorial**, com participação da ANPD, CNJ, Ouvidorias e Conselhos de Direitos Humanos;
- Incluir cláusulas de **revisão periódica e transparência ativa**, obrigando a publicação de métricas de desempenho, relatórios técnicos e mecanismos de prestação de contas.

O PANÓPTICO

@opanopticobr
@opanopticobr
pablo@cesecseguranca.com.br
www.opanoptico.com.br