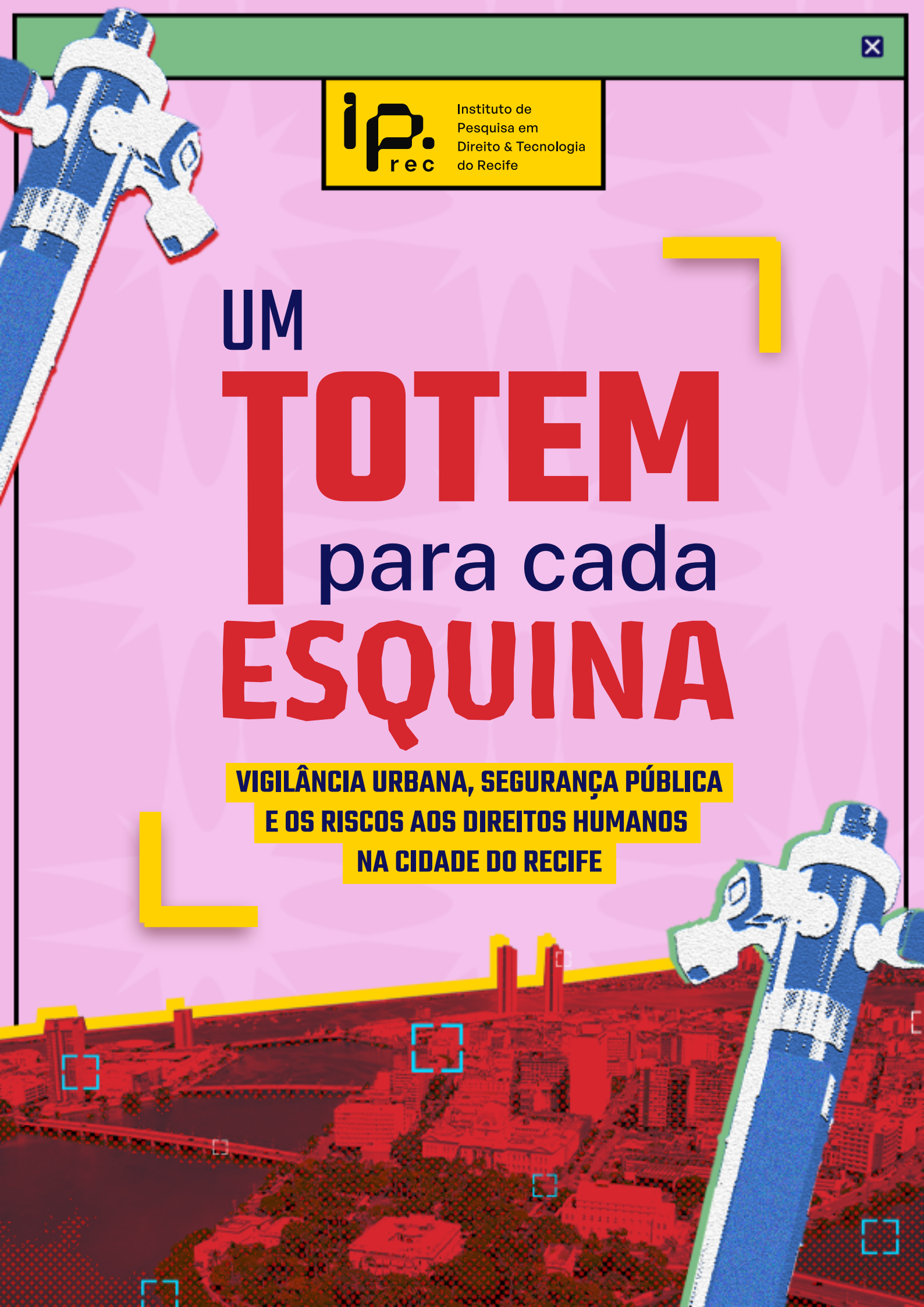




Instituto de
Pesquisa em
Direito & Tecnologia
do Recife

UM TOTEM para cada ESQUINA

**VIGILÂNCIA URBANA, SEGURANÇA PÚBLICA
E OS RISCOS AOS DIREITOS HUMANOS
NA CIDADE DO RECIFE**



Um totem para cada esquina: vigilância urbana, segurança pública e os riscos aos direitos humanos na cidade do Recife

Agosto de 2026

Instituto de Pesquisa em Direito e Tecnologia do Recife – IP.rec

Este relatório integra projeto desenvolvido pelo IP.rec, com apoio financeiro do Fundo de Resposta Rápida (FRR) da Derechos Digitales.

Pesquisa e redação

André Fernandes
Pedro Silva Neto
Helton Leyendecker
Mariana Cavalcanti
Rhaiana Valois

Coordenação e revisão

André Fernandes

Projeto gráfico

Estúdio PUYA!

Este conteúdo está licenciado sob a Creative Commons Atribuição-Não Comercial 4.0 Internacional (CC BY-NC 4.0), permitindo o uso, compartilhamento e adaptação apenas para fins não comerciais, com atribuição à autoria original.

Como citar

FERNANDES, André Lucas; SILVA NETO, Pedro; LEYENDECKER, Helton; CAVALCANTI, Mariana; VALOIS, Rhaiana. Um totem para cada esquina: vigilância urbana, segurança pública e os riscos aos direitos humanos na cidade do Recife. Recife: Instituto de Pesquisa em Direito e Tecnologia do Recife – IP.rec, 2026.



INTRODUÇÃO

Tem-se verificado, mundialmente e no Brasil, a implementação de tecnologias de **reconhecimento facial**. Estima-se que, no mundo, o mercado de reconhecimento facial deverá crescer de US\$ 5,69 bilhões em 2023 para US\$ 12,05 bilhões até 2028, um crescimento agregado de 16,20% durante o período de previsão (2023-2028)¹. Até o momento, foram encontrados 471 casos ativos de uso de RF pelas instituições de segurança pública no país², fora os usos de outras naturezas. Um forte impulso nesse sentido foi a assinatura, em 2019, da portaria no 793, que destinou parte do Fundo Nacional de Segurança Pública para a implementação dessa ferramenta na segurança pública de estados e/ou municípios.

Ao tempo da redação deste relatório, encontra-se em tramitação no Congresso Nacional o Projeto de Lei no 1.828/2023, que propõe autorizar a instalação de sistemas de reconhecimento facial em estações ferroviárias, rodoviárias, vias públicas e repartições públicas. A iniciativa legislativa insere-se em um contexto de intenso debate nacional sobre os limites jurídicos do uso de tecnologias biométricas na segurança pública. Organizações da sociedade civil, reunidas na Coalizão Direitos na Rede³ e na Campanha Tire Meu Rosto da Sua Mira, manifestaram preocupação com a proposta, sustentando que a ampliação do reconhecimento facial carece de salvaguardas adequadas de transparência, governança, proteção de dados e direitos fundamentais, além de questionarem sua efetividade e os riscos de discriminação algorítmica e vigilância massiva.

Pernambuco e sua capital, Recife, permanecem reiteradamente entre os territórios mais afetados pela violência letal no país. Os dados de 2024 do Anuário Brasileiro de Segurança Pública evidenciam a gravidade desse cenário: Pernambuco foi o 4º

1 Fonte: <https://www.mordorintelligence.com/pt/industry-reports/facial-recognition-market>

2 Mapeamento realizado pelo Panóptico. Acesso em 29/10/2025. Disponível em: <https://www.opanoptico.com.br/#mapa>.

3 Fonte: <https://direitosnarede.org.br/2025/09/02/nota-publica-sobre-projeto-de-lei-1828-2023-que-autoriza-o-uso-de-sistemas-de-reconhecimento-facial-em-sistemas-de-transporte-publico-e-reparticoes-publicas>.



estado com a maior taxa de mortes violentas intencionais (MVI) por 100 mil habitantes, registrando 3.453 vítimas. Além disso, o estado concentra dois dos 10 municípios com as maiores taxas de MVI do Brasil: Cabo de Santo Agostinho (73,3) e São Lourenço da Mata (73). No plano das capitais, Recife ocupa a terceira posição na taxa de MVI por 100 mil habitantes (39,1) e a sexta colocação em números absolutos (620). O quadro se agrava quando observadas outras formas de criminalidade patrimonial: Pernambuco figura como o 4º estado em números absolutos de roubos e furtos de veículos e o 6º em números absolutos de roubos e furtos de celulares.

Diante desse cenário catastrófico de insegurança, que pouco oscilou ao longo das últimas décadas, as gestões municipais e estadual sucederam-se na proposição de estratégias capazes de enfrentar os problemas da segurança pública, poucas delas obtendo sucessos duráveis. Com a ascensão da *big data*, da inteligência artificial e do reconhecimento facial nesta década, essas tecnologias têm se tornado a “bola da vez” do enfrentamento ao crime.

Em **Recife**, o tema foi para o centro do debate público com a publicação de um edital, em 2021, que previa a instalação de 108 relógios digitais pela cidade com câmeras de reconhecimento facial. Em 2023, a Secretaria da Educação declarou⁴ a pretensão de adotar sistemas de reconhecimento facial como parte de um plano de segurança integrado para as escolas do estado; além disso, estão em curso o uso de RF para acesso a vários prédios públicos da cidade, assim como os primeiros testes para a implementação em estádios de futebol⁵. O reconhecimento facial, no entanto, apresenta uma série conhecida de problemas e riscos, especialmente no seu uso na segurança pública. O estado de **Pernambuco** tem 62,6% de população negra - uma proporção acima da média nacional⁶ - que seria diretamente impactada, por ser um segmento mais suscetível à imprecisão algorítmica presente no reconhecimento facial. Também é o 5º estado do país com o maior número de homicídios de pessoas trans⁷, também mais suscetível aos vieses.

Recentemente, um novo capítulo tem se descortinado pelas ruas. Dezenas de **totens contendo câmeras de vigilância** têm sido instalados em diversos pontos da cidade - somente pelo projeto LidEye no EITA Labs, são 89⁸. De acordo com a página oficial do

4 Fonte: <https://www.folhape.com.br/noticias/governo-de-pernambuco-planeja-adotar-reconhecimento-facial-em-escolas/265871/>.

5 Fonte: <https://www.sds.pe.gov.br/noticias/11661-pernambuco-tem-novas-medidas-de-seguranca-para-jogos-de-futebol-e-retorno-das-charangas>.

6 Fonte: Dados de 2005. Fonte: <http://produtos.seade.gov.br/produtos/idr/download/populacao.pdf>.

7 Fonte: Dados de 2021. Fonte: <https://agenciabrasil.ebc.com.br/direitos-humanos/noticia/2022-01/brasil-registrou-140-assassinatos-de-pessoas-trans-em-2021#:~:text=Em%20rela%C3%A7%C3%A3o%20C3%A0%20distribui%C3%A7%C3%A3o%20geogr%C3%A1fica,Fran%C3%A7a%20e%20outro%20em%20Portugal>.

8 Informações disponíveis em mapa na página oficial do projeto. Acesso em 29/10/2025. Disponível em: https://www.google.com/maps/d/u/0/viewer?mid=1_DczKWIRu3Eawah8mHlc4ItfysQ1_W0&femb=1&ll=-8.096640753312265%2C-34.886517099999985&z=13.

projeto, trata-se de uma rede colaborativa de segurança⁹ que tem o objetivo de “redução da criminalidade, aumento da segurança e melhoria na gestão estratégica de segurança pública por meio de uma rede colaborativa com totens de vídeo vigilância inteligente, contendo algoritmos de inteligência artificial para monitoramento preventivo e repressivo”¹⁰. Embora a informação sobre a presença de reconhecimento facial nos totens instalados na cidade não esteja presente na apresentação institucional da LidEye nem em matérias da imprensa, essa aplicação é mencionada em postagens tanto da empresa¹¹ quanto do prefeito do Recife, João Campos¹², ambas no Instagram.

A disseminação dos totens de vigilância em Recife parece encontrar guarida experimental no projeto EITA Labs, sandbox regulatório estruturado a partir do Decreto Municipal no 35.511, de 1o de abril de 2022, que instituiu o Recife Living Labs. O decreto estabelece ambientes urbanos experimentais destinados ao teste de soluções tecnológicas voltadas à inovação e ao aperfeiçoamento dos serviços públicos, circunscrevendo sua atuação ao Sítio Histórico do Bairro do Recife (Zona Primária), ao quadrilátero do Bairro de Santo Amaro (Zona Secundária 1) e à Avenida Guararapes e áreas adjacentes (Zona Secundária 2). Embora a lógica do sandbox permita maior flexibilidade regulatória para experimentação, ela também tende a reduzir os mecanismos tradicionais de controle, transparência e prestação de contas, abrindo espaço para uma expansão da vigilância sem o correspondente escrutínio público.

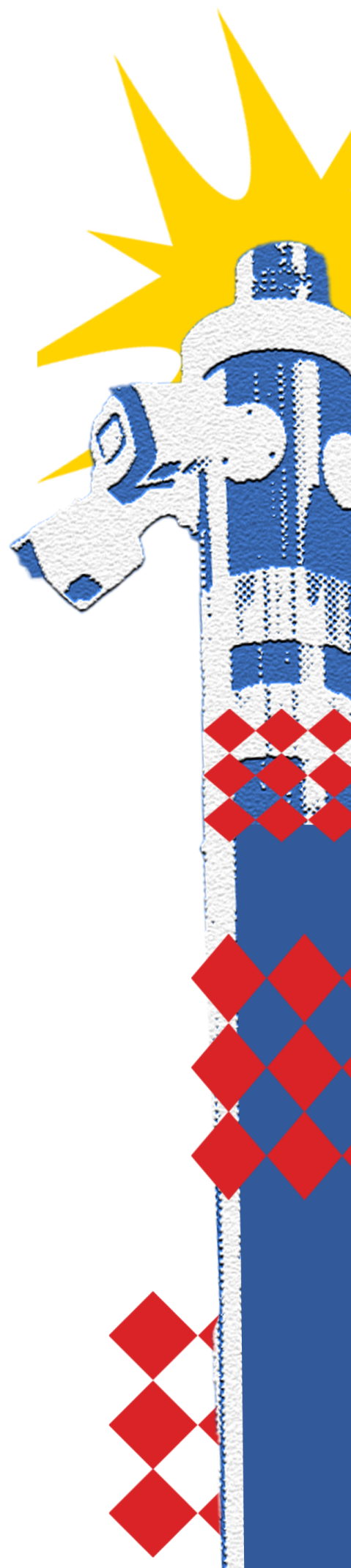
A inexistência de um marco normativo específico, tanto em Recife quanto em Pernambuco, para disciplinar o emprego de sistemas de videomonitoramento com inteligência artificial e reconhecimento facial aprofunda esse cenário, inserindo tais práticas

9 Documento de apresentação do projeto e descrição de seu funcionamento. Acesso em 29/10/2025. Disponível em: <https://drive.google.com/file/d/1Nz-wVLsRDpOcAwoMwXtmwclC3lVQWHL/view?usp=sharing>.

10 Página oficial do projeto, acessível através de QR codes presentes em todos os totens. Acesso em 29/10/2025. Disponível em: <https://sites.google.com/recife.pe.gov.br/eitalabs/solu%C3%A7%C3%B5es-implantadas/2%C2%BA-ciclo-2024/lideye?authuser=0>.

11 Postagem no perfil do Instagram da LidEye mencionando o uso de reconhecimento facial no Recife durante o réveillon 2024-2025. Acesso em 29/10/2025. Disponível em: <https://www.instagram.com/p/DKuKAQmBjQ9/>.

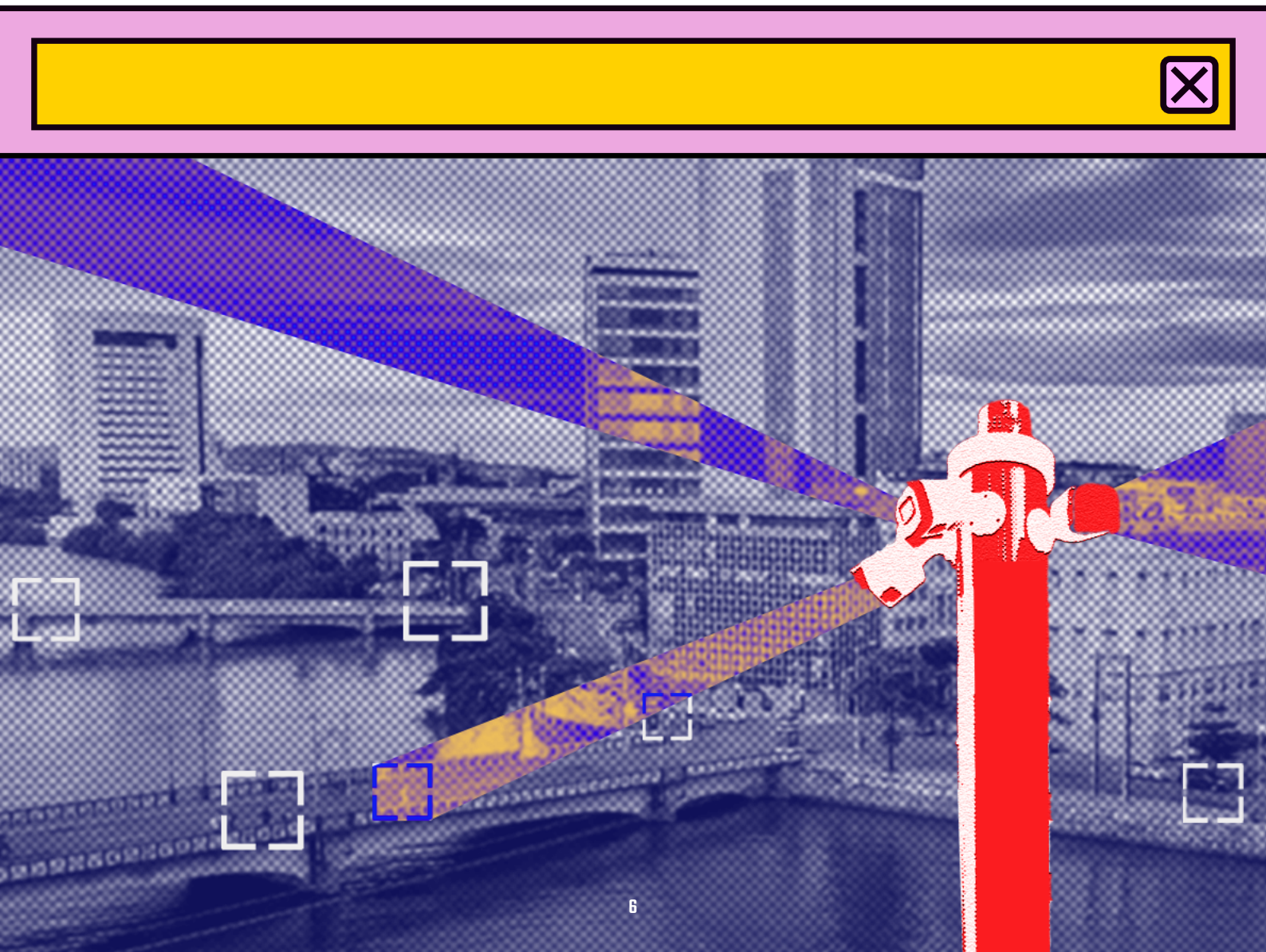
12 Postagem no perfil do Instagram do prefeito João Campos mencionando o uso de reconhecimento facial no Recife durante o carnaval de 2025. Acesso em 29/10/2025. Disponível em: <https://www.instagram.com/reel/DGfxQ4YxZv4/>.



em uma zona de indefinição jurídica que compromete a transparência, o controle social e a própria observância do princípio da legalidade na implementação de políticas públicas.

Soma-se a isso o fato de que o uso dessas tecnologias na segurança pública permanece cercado de controvérsias quanto à sua efetividade, ao mesmo tempo em que pode reproduzir discriminações estruturais e consumir elevados recursos públicos sem resultados proporcionais. Sob essa perspectiva, a atuação dos gestores municipais e estaduais suscita questionamentos quanto à compatibilidade com princípios estruturantes da formulação de políticas públicas, entre eles a legalidade, a participação social, a transparência, a equidade, a avaliação baseada em evidências e a accountability.

Em um contexto marcado pela falta de informações sobre o funcionamento dos torens, os bancos de dados empregados e as empresas responsáveis por sua operação, delineia-se a formação de uma infraestrutura de vigilância pouco transparente, cuja conformidade com a Lei Geral de Proteção de Dados (LGPD), a existência de mecanismos para mitigação de vieses algorítmicos e a própria legitimidade democrática permanecem sem esclarecimento adequado.



METODOLOGIA

A presente pesquisa adotou como estratégia metodológica principal a **utilização da Lei de Acesso à Informação (Lei no 12.527/2011) como instrumento de coleta de dados**. Essa opção mostrou-se especialmente adequada em razão de duas circunstâncias. A primeira decorre do fato de que a Prefeitura do Recife possui um sistema estruturado para recebimento e processamento de pedidos de acesso à informação, aliado a uma política relativamente consolidada de transparência ativa e dados abertos. A segunda reside na própria natureza do objeto investigado. Os sistemas de videomonitoramento analisados encontravam-se inseridos no âmbito do programa EITA! Labs, sandbox regulatório instituído pelo Decreto Municipal no 35.511/2022, circunstância que sujeita sua implementação e acompanhamento à atuação da Administração Pública e, conseqüentemente, aos deveres de publicidade e transparência decorrentes do regime jurídico administrativo.

Esse aspecto possui relevância metodológica. Caso a investigação tivesse por objeto exclusivamente sistemas privados de vigilância, sem qualquer vínculo com políticas públicas ou ambientes regulatórios estatais, a obtenção das informações dependeria essencialmente da colaboração voluntária das empresas responsáveis, inexistindo dever jurídico equivalente de prestação de informações. A inserção da solução tecnológica em um sandbox regulatório municipal permitiu, portanto, que a pesquisa utilizasse mecanismos formais de acesso à informação para examinar aspectos técnicos, jurídicos e institucionais relacionados ao projeto. Este, portanto, é um projeto piloto de análise, voltado ao Poder Público. A debilidade da pesquisa-ação aqui se mostra no fato de que boa parte das mesmas estruturas tem se espalhado pela cidade em iniciativas exclusivamente privadas, o que torna ainda mais complexo o cenário de transparência e governança quando ausente um regramento específico.

A etapa de construção dos instrumentos de coleta consistiu na elaboração de um conjunto abrangente de perguntas voltadas a diferentes dimensões da implantação dos "sistemas de video-



monitoramento inteligente”. Para facilitar sua organização, as questões foram distribuídas em grupos temáticos identificados pelas letras A, B, C, D, E, F, G, H, I, J e K. Cada eixo temático foi atribuído a um pesquisador ou pesquisadora responsável por sua elaboração e revisão técnica, buscando assegurar coerência interna entre as perguntas, evitar sobreposições e garantir que cada conjunto de quesitos fosse capaz de produzir informações relevantes para os objetivos específicos da pesquisa.

Em razão das limitações de caracteres existentes no formulário eletrônico utilizado pela Prefeitura do Recife para apresentação dos pedidos de acesso à informação, foi necessário consolidar e sintetizar as perguntas originalmente elaboradas. Essa restrição influenciou diretamente a organização metodológica adotada, exigindo a reunião de quesitos por afinidade temática e sucessivos ajustes redacionais para permitir o envio integral das solicitações sem perda significativa de conteúdo - assim resultando na estrutura de “duas letras” relatada abaixo.

Os pedidos foram protocolados separadamente por grupo temático. Em linhas gerais, as respostas iniciais apresentadas pela Administração Pública seguiram padrão semelhante entre os diferentes eixos analisados, caracterizando-se por respostas genéricas, remissões a documentos previamente conhecidos e ausência de enfrentamento individualizado de diversos questionamentos formulados. Em numerosos casos, tampouco houve declaração expressa da inexistência das informações solicitadas, providência importante para eliminar ambiguidades e permitir adequada interpretação dos resultados da pesquisa.

Diante dessas insuficiências, foram interpostos recursos administrativos em primeira instância, buscando complementar as informações fornecidas, esclarecer omissões e obter acesso aos documentos mencionados nas respostas iniciais. Em diversos casos, essa etapa resultou na disponibilização de novos documentos e esclarecimentos adicionais, posteriormente analisados nos capítulos específicos deste relatório.

Persistindo lacunas relevantes, foram apresentados recursos administrativos em segunda instância, permitindo o aprofundamento da coleta documental e a obtenção de novas informações que igualmente subsidiaram as análises desenvolvidas ao longo deste estudo.

Ao término da tramitação dos recursos administrativos, foi elaborado um levantamento consolidado das informações e documentos que permaneceram pendentes de apresentação pela Administração Pública.

Após a coleta documental, foi realizada uma análise qualitativa de conteúdo das respostas administrativas, contratos, atas, termos de confidencialidade, planos operacionais e demais documentos disponibilizados pela Prefeitura do Recife e pela EMPREL. A análise buscou identificar padrões de resposta, omissões recorrentes, inconsistências entre documentos, evolução das informações ao longo das instâncias recursais e o grau

de aderência das respostas às exigências da Lei de Acesso à Informação (LAI) e da Lei Geral de Proteção de Dados (LGPD).

Para fins analíticos, os dados foram organizados segundo os mesmos eixos temáticos utilizados na coleta (AB, CD, EF, GH, IJ e K), permitindo examinar separadamente: (i) a base normativa e a transparência da implantação; (ii) o processo decisório e a governança contratual; (iii) a infraestrutura tecnológica e o funcionamento dos sistemas; (iv) a integração institucional e a governança de dados; (v) os mecanismos de controle, monitoramento e avaliação; e (vi) as salvaguardas de governança ética da inteligência artificial.

Em cada eixo, procedeu-se à comparação entre os pedidos formulados, as respostas iniciais, os recursos administrativos e os documentos efetivamente disponibilizados, com o objetivo de verificar: a existência ou inexistência das informações solicitadas; o nível de detalhamento fornecido; a consistência entre diferentes manifestações da Administração; e a presença de elementos mínimos de transparência, prestação de contas e avaliação de riscos. Também foram examinadas as justificativas utilizadas para negar acesso a informações, especialmente aquelas baseadas em alegações de sigilo comercial, propriedade intelectual ou segurança pública.

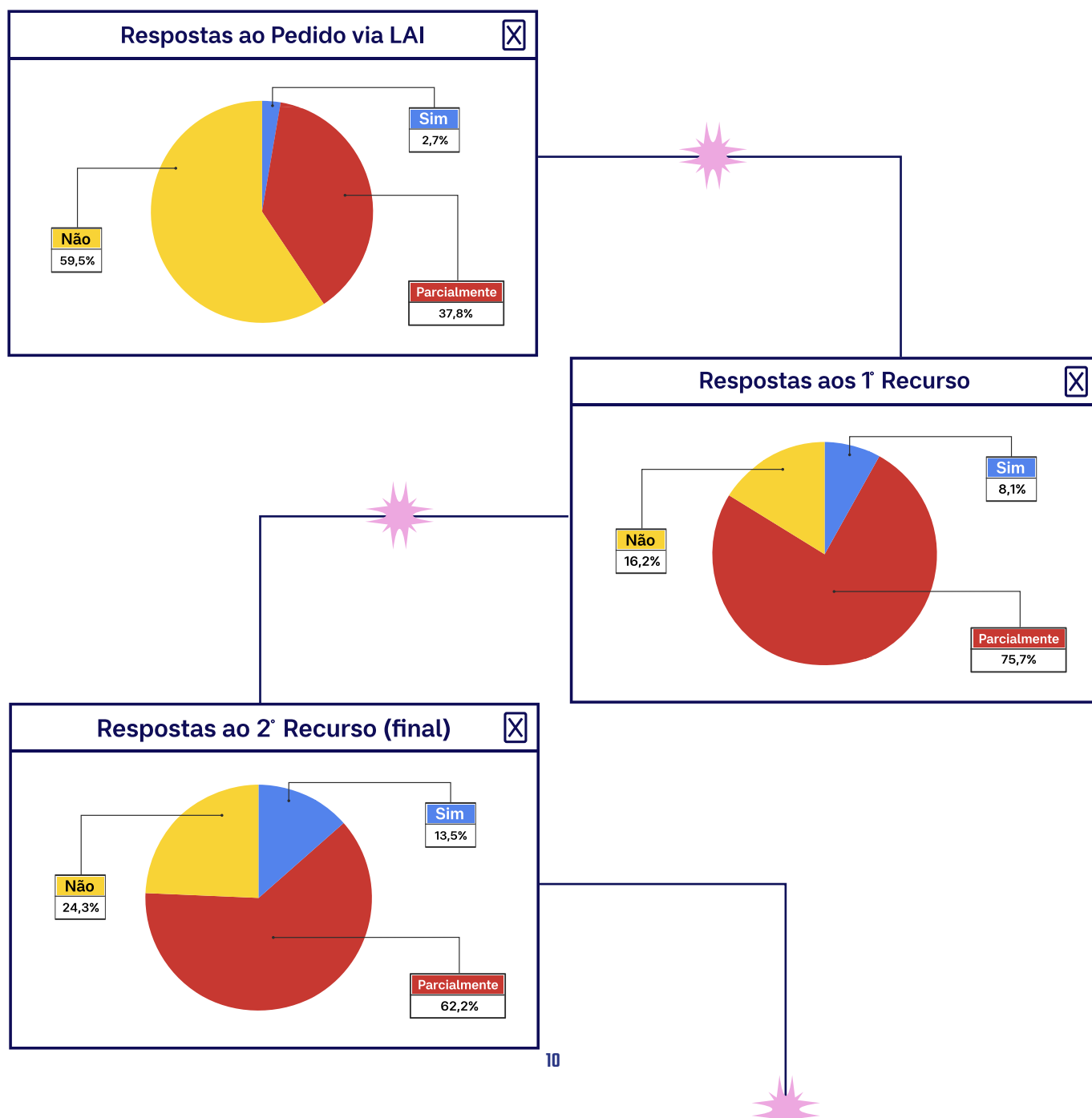
O enfoque adotado foi predominantemente jurídico-institucional e de governança pública, buscando compreender não apenas o conteúdo técnico da solução tecnológica, mas também as condições de sua implementação, supervisão, transparência e compatibilidade com direitos fundamentais em contexto de vigilância urbana.

Por fim, a partir do diagnóstico produzido ao longo da pesquisa, o relatório apresenta, em caráter de anexo, um conjunto de recomendações voltadas ao aprimoramento da governança do uso de tecnologias de videomonitoramento inteligente no âmbito municipal. As propostas foram elaboradas sob uma perspectiva multissetorial, buscando compatibilizar inovação tecnológica, segurança pública e proteção de direitos fundamentais, à luz da Lei Geral de Proteção de Dados (LGPD), da legislação de acesso à informação, dos princípios constitucionais aplicáveis à Administração Pública e das principais referências nacionais e internacionais sobre governança, ética e uso responsável da inteligência artificial. As recomendações contemplam medidas relacionadas à transparência, prestação de contas, avaliação de impacto, governança de dados, supervisão humana, mitigação de vieses algorítmicos, participação social, auditoria e fortalecimento dos mecanismos institucionais de controle, oferecendo subsídios para a formulação de políticas públicas mais legítimas, responsáveis e orientadas por evidências.

No momento da redação deste relatório, encontrava-se em andamento a abertura de um canal complementar de diálogo com a Prefeitura do Recife para tentativa de obtenção dessas informações por meio de interlocução direta, para além do procedimento formal da Lei de Acesso à Informação. Em resposta ao conjunto consolidado de questionamentos encaminhado pelo IP.rec, a Prefeitura reafirmou que as manifestações

e recursos apresentados no âmbito da LAI teriam sido respondidos integralmente dentro dos prazos legais, informou que o Relatório ISES encontrava-se em fase final de homologação e reiterou a disposição para manutenção de diálogo institucional, inclusive por meio de oficinas de trabalho e reuniões técnicas.

Todavia, a manifestação não enfrentou individualmente as lacunas apontadas nem apresentou os documentos e informações específicos cuja ausência havia sido destacada pelo IP.rec. Permaneceram sem resposta satisfatória diversos questionamentos relativos, entre outros aspectos, ao processo administrativo integral do projeto, estudos prévios de impacto, instrumentos de governança, documentação técnica, políticas de tratamento de dados, avaliações de risco, mecanismos de auditoria e demais documentos requeridos. Dessa forma, embora a interlocução institucional tenha permanecido aberta, a resposta apresentada não alterou substancialmente as conclusões deste relatório quanto às insuficiências de transparência identificadas ao longo da pesquisa.



ANÁLISE

AB. Base normativa e transparência na implantação dos sistemas

Com o objetivo de examinar o arcabouço normativo e a transparência na implantação do projeto LidEye, os pedidos iniciais de acesso à informação buscaram obter: (i) os atos normativos que regulam o sandbox do EITA!Labs, incluindo decretos, portarias e mapas de perímetro; (ii) as regras e procedimentos aplicáveis a soluções de vigilância/segurança, abrangendo critérios de seleção, requisitos de transparência e salvaguardas técnicas; (iii) a composição, pautas, atas e deliberações do Conselho Gestor e do Comitê Coordenador do Programa “Recife Living Labs” (CCRLL) referentes ao projeto; (iv) documentos sobre o critério territorial, como a delimitação do sandbox e justificativas para instalação de totens fora do perímetro oficial; (v) a documentação relacionada à renovação contratual e à continuidade do projeto em 2026; (vi) informações sobre a existência de página de transparência ativa do EITA!Labs; e (vii) estudos, pareceres e notas técnicas produzidos previamente à instalação, avaliando necessidade, proporcionalidade, impactos em direitos fundamentais e conformidade com a LGPD, a Constituição Federal e o ECA Digital.

Em sua primeira manifestação, a Prefeitura do Recife, por meio da Secretaria de Transformação Digital, Ciência e Tecnologia (SECTI), forneceu uma descrição genérica do programa EITA!Labs e do projeto LidEye, inserido no 2o Ciclo do sandbox regulatório municipal. Foram disponibilizados links para o Edital de Chamamento, o Decreto Municipal no 35.511/2022, o Termo de Confidencialidade firmado com a empresa e o Contrato AJU no 035/2024. A resposta limitou-se a informar que as câmeras possuem capacidade de reconhecimento facial “embarcada”, mas que tal funcionalidade não estava em operação, e que estavam sendo testados apenas “outros analíticos de vídeo” não relacionados à biometria.

Com base nisso, a SECTI declarou a inexistência de Relatórios

de Impacto à Proteção de Dados (RIPD) ou de estudos de viés étnico-racial e de gênero, afirmando que os riscos da experimentação estariam “resguardados por Termo de Confidencialidade firmado com a empresa parceira, além do acompanhamento contínuo do COP”. Acrescentou que as câmeras não constantes na lista, no portal oficial, dos 88 totens instalados, seriam de competência da Secretaria de Desenvolvimento Urbano e Licenciamento (SEDUL). Outros documentos administrativos solicitados como atas do Conselho Gestor, estudos pré-instalação, justificativas técnicas para a expansão territorial ou registros de renovação contratual, não foram apresentados.

Em sede de recurso, sustentou-se que a resposta não atendeu integralmente aos pedidos, limitando-se a explicações genéricas e à juntada de documentos isolados, sem fornecer os registros administrativos requeridos. Argumentou-se que a oposição de sigilo comercial à publicidade das salvaguardas previstas no Decreto no 35.511/2022 seria juridicamente insubsistente, pois o Termo de Confidencialidade regula segredos industriais entre a EMPREL e a contratada, mas não substitui os pareceres técnicos de impacto à privacidade e as medidas de proteção devidas à coletividade, especialmente diante da presença de hardware de reconhecimento facial em áreas de circulação de crianças e adolescentes – risco potencial cujo estudo de mitigação deveria ser público.

Apontou-se ausência da Ata de Reunião do Conselho Gestor, expressamente citada no Contrato, e dos conteúdos exigidos pelo art. 6º, IV do Decreto. Quanto à execução, requereu-se esclarecimento formal sobre a operação de 41 totens fora do perímetro delimitado sem o devido ato/pedido de adequação territorial, bem como sobre a validade jurídica da continuidade do projeto em 2026, uma vez que o contrato expirara em dezembro de 2025 sem termo aditivo que justificasse a prorrogação.

Em resposta, a SECTI apresentou novos esclarecimentos e anexou novos documentos. Sobre a vigência, afirmou que o Contrato AJU no 035/2024 não foi renovado e que a empresa fora notificada para desmobilizar os equipamentos, nos termos do Plano de Mobilização e Desmobilização. A justificativa para os 41 totens fora do perímetro original foi ancorada na Ata de Reunião no 03/2024 do Conselho Gestor, que autorizou a expansão para validação em segurança patrimonial e grandes eventos, notadamente Réveillon e Carnaval de 2025, a pedido da Secretaria de Ordem Pública e Segurança. No tocante ao reconhecimento facial, insistiu na tese de que a funcionalidade permaneceu inativa e que a obrigação de elaborar RIPD “vincula-se ao tratamento efetivo de dados biométricos”, de modo que a mera capacidade do hardware não configuraria fato gerador para o relatório. Foram, então, disponibilizados links para a Ata no 03/2024 (sobre a aprovação inicial da solução), a Ata no 01/2025 (sobre realocação e expansão) e o Plano de Mobilização e Desmobilização, considerando a administração que o pedido fora integralmente satisfeito.

Em novo recurso, sobre a desmobilização e a territorialidade, apontou-se que os links

fornecidos para o Plano de Mobilização e para as Atas do Conselho Gestor exigiam solicitação de acesso, não estando abertos à consulta pública, em inobservância às obrigações de transparência ativa (art. 8º, LAI) e impedia verificar se a desmobilização estava efetivamente prevista ou em curso. No mérito do tratamento de dados, demonstrou-se a insubsistência do argumento de que a inatividade do reconhecimento facial afastaria a necessidade de RIPD.

Citou-se o formulário de inscrição da LidEye no 2º ciclo do EITA!Labs, no qual a empresa, ao ser questionada se a solução necessitaria de espaço de experimentação urbano, respondeu: “Sim, é necessário espaços urbanos para as câmeras serem instaladas e testadas, assim como, gerar material para a elaboração de relatórios, aprendizados de máquina, analíticos e a captação e tratamento desses dados (cenas reais e cenas suspeitas)”. Ora, se a captação e o tratamento de dados foram assumidos como necessários ao experimento, o tratamento de dados pessoais estava configurado, e o RIPD era devido, independentemente do acionamento do módulo biométrico.

A manifestação final da Prefeitura limitou-se a informar que os acessos aos documentos restritos haviam sido “devidamente liberados” e que o Relatório ISES estava sendo finalizado pela equipe técnica, para posterior homologação pelo Conselho do EITA!Labs. Nenhum dos documentos de fundo solicitados — estudos pré-instalação, RIPD, ato formal de criação da TEIA — foi efetivamente apresentado. A experiência evidencia um sandbox regulatório que operou sem estudos públicos prévios, sem documentação acessível de suas deliberações e sem mecanismos verificáveis de prestação de contas.

CD. Processo decisório, governança contratual e arranjos institucionais

Neste tópico, buscou-se obter transparência sobre a participação da solução LidEye no EITA Labs, abrangendo todas as etapas de submissão, avaliação, aprovação e acompanhamento do projeto. Para isso, foi requerida a cópia integral do processo administrativo e de seus apensos, incluindo inscrições, análises de elegibilidade, atas e registros de reuniões, apresentações, relatórios, comunicações internas e eventuais autorizações relacionadas à implementação da solução. Também foram solicitadas informações sobre o número do processo, a unidade administrativa responsável, os agentes encarregados da fiscalização e a cadeia de aprovações institucionais envolvida.

O pedido buscou acessar ainda contratos, termos de parceria, convênios, aditivos e demais instrumentos eventualmente firmados entre a Prefeitura do Recife, a Emprel, o EITA Labs e a empresa LidEye, a fim de compreender as bases jurídicas e operacionais do projeto, especialmente quanto ao objeto, escopo, prazos, obrigações das partes, cláusulas de confidencialidade, propriedade intelectual, tratamento de dados, segurança da informação e adequação à Lei Geral de Proteção de Dados Pessoais (LGPD).

Além disso, o requerimento procurou identificar a existência de custos públicos diretos ou indiretos associados ao projeto, bem como eventuais possibilidades de exploração comercial da solução pela empresa participante. Nesse contexto, foram solicitadas planilhas de custos, documentos de custeio, comprovantes de utilização de infraestrutura pública e registros de pagamentos, cessões ou quaisquer formas de apoio fornecidas pela administração pública. Por fim, buscou-se esclarecer se a LidEye poderia explorar comercialmente a tecnologia durante ou após o período de sandbox de inovação, incluindo as condições, limitações e salvaguardas previstas nos documentos administrativos e contratuais.

Na primeira resposta ao pedido, não houve a apresentação integral do processo administrativo solicitado. A administração disponibilizou apenas o edital de chamamento público para credenciamento, o contrato firmado e o acordo de confidencialidade, sem encaminhar os documentos referentes à tramitação administrativa da submissão, avaliação, aprovação e acompanhamento da solução LidEye no âmbito do EITA Labs. Também não foram fornecidas informações completas acerca da cadeia de aprovações, comunicações internas, relatórios de acompanhamento e demais registros administrativos requeridos.

Em relação aos instrumentos contratuais, verificou-se igualmente a ausência de partes integrantes do contrato, permanecendo pendente a apresentação do plano de mobilização e desmobilização, bem como da Ata de Reunião no 3/2024 do Conselho Gestor do Programa Recife Living Labs. Quanto aos custos do projeto, a resposta limitou-se à afirmação genérica de que “não há custos para a Prefeitura do Recife, sendo a instalação, manutenção e desmobilização integralmente custeadas pela proponente”, sem o envio de documentos comprobatórios, planilhas, registros administrativos ou elementos capazes de demonstrar a inexistência de custeio público direto ou indireto.

No que diz respeito à exploração econômica da solução, a resposta informou que, durante o período do sandbox, em regra, não pode haver exploração comercial da tecnologia, admitindo-se apenas eventual cobrança destinada à cobertura de custos de manutenção da experimentação, desde que previamente submetida à consulta e aprovada pelo CCRLL e pelo Conselho Gestor, nos termos da cláusula 5.6 contratual. Contudo, não houve esclarecimento específico acerca da exploração comercial posterior ao encerramento do sandbox, inexistindo previsão expressa de vedação ou autorização automática para utilização econômica futura da solução.

Diante dessas omissões, foi interposto o primeiro recurso administrativo sustentando que a resposta apresentada não atendeu integralmente ao pedido formulado. Nele destacou-se que a juntada isolada do edital, contrato e acordo de confidencialidade não substitui a apresentação do processo administrativo regularmente constituído, especialmente porque a própria existência do contrato pressupõe a produção de atos ad-

ministrativos prévios, como análises, pareceres, comunicações internas e aprovações institucionais. Também foi apontada a ausência de informações objetivas indispensáveis ao controle administrativo, bem como a não disponibilização integral dos documentos contratuais e de seus anexos.

Em relação aos custos e custeio do projeto, argumentou-se que a mera declaração de inexistência de despesas para a Prefeitura não supre a obrigação de apresentação documental prevista na LAI. Por essa razão, requereu-se o provimento do recurso para que fossem fornecidos integralmente os documentos solicitados ou, havendo restrição de acesso, apresentada justificativa específica e fundamentada, nos termos do art. 7º, §2º, da Lei no 12.527/2011.

Em resposta ao recurso interposto, a Secretaria de Transformação Digital, Ciência e Tecnologia (SECTI) anexou outros documentos internos relacionados ao projeto LidEye. Entre os documentos apresentados, constaram o formulário de submissão da empresa, a Ata de Reunião no 03/2024 do Conselho Gestor, responsável por formalizar a aprovação da solução e registrar discussões sobre acurácia dos alertas e integração com o Centro de Operações do Recife (COP), a Ata da Reunião no 01/2025, relativa à autorização para realocação e expansão perimetral da solução, o Contrato de Experimentação AJU no 035/2024 e o Plano de Mobilização e Desmobilização, contendo informações sobre a retirada dos equipamentos ao término da experimentação.

A administração também esclareceu que a unidade responsável pela gestão e acompanhamento técnico da experimentação seria a Diretoria de Inovação Aberta e Governança (DIAG) da Emprel. Segundo a resposta, a fiscalização do contrato ocorreria de forma colegiada pelo Conselho Gestor do EITA Labs e pelo CCRL, além do acompanhamento técnico realizado por gestores designados pela própria Emprel, nos termos das cláusulas previstas no Contrato AJU no 035/2024. Com isso, a Prefeitura buscou responder aos questionamentos referentes à identificação dos responsáveis institucionais pela condução e supervisão do projeto.

Quanto aos custos e ao custeio da iniciativa, a SECTI afirmou que não existem notas de empenho, ordens de pagamento ou registros de transferência financeira relacionados ao projeto, sob o argumento de que o modelo de sandbox do EITA Labs, previsto no Decreto Municipal no 35.511/2022 e no Edital no 003/2024, estabelece que a empresa proponente assume integralmente os riscos e custos da experimentação. A resposta destacou que, conforme previsto no Plano de Mobilização e Desmobilização, a empresa LidEye seria a única responsável pelos custos de conectividade e energia elétrica dos totes instalados, cabendo ao Município apenas a cessão gratuita do espaço público para realização dos testes. Em razão da natureza não onerosa da parceria, a administração declarou formalmente a inexistência de faturas, notas fiscais ou quaisquer documentos relativos a fluxo de caixa público vinculado ao projeto.

Por fim, diante da persistência das omissões identificadas, foi interposto segundo recurso administrativo, sustentando a insuficiência material da resposta apresentada pela administração pública. O recurso apontou que, embora tenham sido juntados alguns documentos isolados (como formulário de submissão, contrato e acordo de confidencialidade), continuou ausente a cópia integral do processo administrativo formalmente autuado, com encadeamento cronológico dos atos praticados, incluindo análises, pareceres, comunicações internas, relatórios e demais registros capazes de demonstrar o fluxo decisório relacionado à participação da solução LidEye no EITA Labs. Argumentou-se que a apresentação fragmentada de documentos não se confunde com o acesso efetivo ao processo administrativo completo.

O recurso também destacou que os próprios documentos encaminhados pela administração fazem referência a anexos e registros integrantes que não teriam sido integralmente disponibilizados, comprometendo a compreensão adequada do procedimento administrativo. Além disso, apesar da identificação da Diretoria de Inovação Aberta e Governança (DIAG/EMPREL) como unidade responsável pela gestão do projeto, a resposta permaneceu genérica quanto à individualização dos responsáveis técnicos, do fiscal do contrato ou termo e da cadeia formal de aprovações administrativas. Em relação aos custos e custeio da iniciativa, sustentou-se que a administração limitou-se a afirmar a inexistência de custos diretos, sem apresentar documentação apta a demonstrar eventuais formas de custeio indireto, como cessão de espaço público, utilização de infraestrutura estatal ou apoio operacional relacionado à experimentação.

O segundo recurso apontou ainda a ausência de manifestação específica acerca da possibilidade de exploração comercial da solução e de eventuais benefícios econômicos decorrentes do projeto. Também foi registrado que os links disponibilizados pela Prefeitura permaneciam com acesso restrito, impedindo a consulta aos documentos indicados e configurando obstáculo indevido ao exercício do direito de acesso à informação. Diante disso, requereu-se novamente o fornecimento integral dos documentos e esclarecimentos solicitados, com acesso efetivo e irrestrito aos arquivos mencionados.

Em resposta, a administração limitou-se a informar genericamente que todos os acessos aos documentos anteriormente apontados como restritos teriam sido devidamente liberados, sem enfrentar de forma específica as demais questões suscitadas no recurso. No plano de desmobilização, que teve acesso liberado posteriormente, foram identificadas funcionalidades analíticas de alta sensibilidade, incluindo biometria facial, contagem de pessoas, detecção de anomalias, detecção de perímetro, reconhecimento de placas de veículos (LPR) e identificação de usuários de veículos suspeitos.

Também foi informada a utilização da plataforma web Monuv, com acesso a dashboard operacional, visualização em tempo real, gravações e relatórios analíticos, além de operação contínua em regime de monitoramento 24/7 e alegada conformidade com a

LGPD. Contudo, a descrição das funcionalidades emprega termos amplos e tecnicamente vagos, como “detecção de anomalias” e “usuários suspeitos”, sem qualquer delimitação objetiva sobre critérios, parâmetros de classificação, bases de dados utilizadas, níveis de acurácia, hipóteses de tratamento de dados ou mecanismos de auditoria e controle.

A previsão expressa de “biometria facial” e a integração operacional com monitoramento contínuo levantam questionamentos relevantes sobre a real extensão das capacidades dos totens instalados e sobre a possibilidade concreta de utilização da infraestrutura para reconhecimento facial, ainda que essa finalidade não tenha sido explicitamente detalhada nos documentos públicos. Isso porque funcionalidades de biometria facial podem abranger desde autenticação e identificação até rastreamento e comparação automatizada de indivíduos em bases de dados, atividades que apresentam elevado risco de vigilância massiva, discriminação algorítmica e produção de falsos positivos.

Além disso, a simples menção à “compliance com LGPD” não é suficiente para demonstrar conformidade material com a legislação, sobretudo diante da falta de informações sobre relatórios de impacto e critérios efetivos de supervisão do sistema.

EF. Infraestrutura tecnológica e funcionamento dos sistemas de vigilância

Com o objetivo de compreender a infraestrutura tecnológica e o funcionamento dos sistemas de vigilância implantados, os pedidos deste eixo buscaram obter as especificações técnicas dos totens e câmeras, a arquitetura de processamento e armazenamento dos dados, os protocolos operacionais, a lista completa dos algoritmos e analíticos de vídeo utilizados, informações sobre o uso de reconhecimento facial e de bases de comparação biométrica, bem como os respectivos estudos de impacto e métricas de desempenho.

Em sua primeira manifestação, a Prefeitura reiterou que o projeto LidEye integrava o 2o Ciclo do EITA!Labs, executado sob o Decreto Municipal no 35.511/2022 e sem custos para o município. Sobre os aspectos técnicos, confirmou que as câmeras possuíam capacidade de reconhecimento facial “embarcada”, mas que tal recurso não se encontrava em operação, e que estavam sendo testados apenas “outros analíticos de vídeo” de caráter experimental e limitado. Com base nessa inatividade, declarou a inexistência de Relatórios de Impacto à Proteção de Dados (RIPD) e de estudos de viés étnico-racial e de gênero, sustentando que os riscos da experimentação estariam “resguardados por Termo de Confidencialidade firmado com a empresa parceira, além do acompanhamento contínuo do COP”. Foram disponibilizados links para o Edital de Chamamento, o Decreto, o Termo de Confidencialidade e o Contrato AJU no 035/2024.

Contudo, a resposta silenciou sobre as especificações técnicas solicitadas – resolu-

ção, visão noturna, captação de áudio, conectividade, retenção, logs de acesso, arquitetura de processamento e localização dos servidores –, bem como sobre a listagem dos analíticos, seus parâmetros e protocolos operacionais. Nenhum diagrama, manual ou descrição de fluxo de dados foi entregue. A administração remeteu ao portal oficial para a lista de totens, mas as informações requeridas não constavam da página indicada.

Em sede de recurso, apontou-se que a resposta não atendeu aos pedidos, limitando-se a remissões insuficientes e a omissões que violavam o art. 6º, IV do Decreto nº 35.511/2022 e a LGPD. Destacou-se que o portal oficial não continha as capacidades do hardware nem informações sobre governança dos dados, e que não foram fornecidos diagramas de fluxo, arquitetura de processamento, localização física do armazenamento ou protocolos operacionais. A menção contratual à “análise em tempo real” não descrevia quais comportamentos geravam alertas, e a recusa em listar os analíticos em teste configurava descumprimento da obrigação de transparência sobre as técnicas experimentais.

Quanto ao reconhecimento facial, argumentou-se que a confirmação da presença da tecnologia “embarcada”, ainda que inativa, não eximia a administração de apresentar estudos de impacto, sobretudo diante do objetivo declarado do projeto no portal do EITA!Labs de “validar sua eficácia na redução da criminalidade [...] por meio de uma rede colaborativa com totens de vídeo vigilância inteligente, contendo algoritmos de inteligência artificial para monitoramento preventivo e repressivo”. Reiterou-se, assim, o pedido de acesso integral às especificações técnicas, à arquitetura de dados, à lista completa dos analíticos em teste e aos estudos de impacto relacionados à funcionalidade de reconhecimento facial.

Em resposta, a SECTI forneceu informações técnicas não constantes na resposta inicial. Descreveram-se dois modelos de totens – Modelo A, com câmera IP Full HD e sistema de áudio; Modelo B, com câmera 4MP 4K, sistema de áudio bidirecional e luz de alerta –, ambos dotados de visão noturna infravermelha. Informou-se que o processamento ocorria em nuvem, pela plataforma Monuv, com retenção de imagens por 7 dias e descarte sob responsabilidade da empresa. Foram listados os analíticos de vídeo em teste: contagem de pessoas, detecção de perímetro, reconhecimento de placas (LPR) e detecção de anomalias (aglomeração atípica e pichação). Acerca do reconhecimento facial, reiterou-se a inatividade e a inexistência de RIPD e de bases de comparação. Invocou-se sigilo comercial e industrial para negar acesso a diagramas de arquitetura e códigos-fonte, argumentando que a administração não detém a propriedade intelectual das tecnologias testadas.

Apesar do avanço, a resposta permaneceu lacônica em pontos sensíveis: não esclareceu se houve efetiva captação de áudio pelos totens, limitando-se a mencionar a existência do hardware; a lista de analíticos foi apresentada sem parâmetros técnicos,

limiares de acionamento ou métricas de avaliação; e o tratamento de imagens por IA em nuvem, fato gerador inequívoco de obrigações sob a LGPD, continuou desacompanhado de RIPD.

Em novo recurso, apontou-se que os analíticos listados eram genéricos e que a ausência de parâmetros como limiares de alerta e critérios definidores de “anomalia” subtraía do cidadão o direito de saber como seu comportamento era interpretado por algoritmos no espaço público. Argumentou-se que o sigilo comercial alegado para os diagramas de arquitetura não impedia a divulgação de um fluxo simplificado de dados, indispensável ao controle social, sobretudo porque a retenção e o descarte ficavam a cargo exclusivo da empresa, sem mecanismos públicos de auditoria. Reiterou-se que o tratamento de imagens por analíticos de vídeo em nuvem constitui fato gerador para a elaboração de RIPD, independentemente da inativação do módulo de reconhecimento facial, e que esse documento jamais foi apresentado. Por fim, registrou-se que o sandbox regulatório tem por finalidade a validação de eficácia, mas nenhum resultado ou avaliação, ainda que preliminar, havia sido disponibilizado ao público, frustrando o dever de prestação de contas. Requereu-se, assim, a apresentação de parâmetros detalhados dos analíticos, de um fluxo de dados simplificado e da avaliação de resultados.

A última resposta da Prefeitura nessa questão não enfrentou nenhum dos pontos remanescentes. Limitou-se a agradecer pelas contribuições e a reiterar que o sandbox também servia para “testar e aprimorar modelos de governança e transparência junto ao cidadão”. Seguiu-se uma nota protocolar sobre os canais adequados para denúncias e reclamações e um alerta, baseado na Súmula CGAI no 01/2016, de que recursos não deveriam ser utilizados para especificações da solicitação inicial, sendo necessário novo pedido para informações adicionais. Com esse encerramento burocrático, a administração deixou sem resposta as questões centrais: o fluxo de dados permaneceu opaco; os parâmetros dos analíticos não foram detalhados; o RIPD jamais foi produzido; e a efetiva utilização do sistema de áudio bidirecional continuou ignorada. A experiência revela um padrão de resistência à transparência que, sob o manto da proteção da propriedade intelectual e de um entendimento restritivo da LAI, manteve a sociedade civil alheia ao funcionamento concreto de uma infraestrutura de vigilância algorítmica instalada em seus espaços de circulação.



Este ponto teve como objetivo apurar a eventual integração do sistema com órgãos municipais, como Guarda Municipal, Secretaria de Segurança Cidadã e CTTU, bem como com órgãos estaduais vinculados à Secretaria de Defesa Social e às polícias militares. Além disso, buscou-se esclarecer o enquadramento jurídico do projeto à luz da LGPD, especialmente quanto à definição dos agentes de tratamento e à identificação de controlador e operador em cada etapa da cadeia de tratamento de dados, envolvendo Prefeitura do Recife, EMPREL, EITA Labs, LidEye e eventuais terceiros participantes.

Para tanto, requereu-se o envio de convênios, termos de cooperação, atos autorizativos, fluxos de compartilhamento de dados e definição dos perfis de acesso vinculados ao tratamento das informações. Também foram solicitados registros de acesso e compartilhamento, incluindo logs anonimizados, relatórios de auditoria e documentação referente ao uso da tecnologia em eventos públicos, como Carnaval e Réveillon, abrangendo plano operacional, métricas, escopo de utilização e relatórios posteriores de avaliação.

No mesmo contexto, pleiteou-se a disponibilização de Relatórios de Impacto à Proteção de Dados (RIPD) relacionados ao programa EITA Labs, ao sandbox físico de vigilância e ao projeto LidEye, além de políticas de privacidade, retenção e descarte de dados, classificação da informação, plano de resposta a incidentes, plano de segurança da informação e identificação do encarregado pelo tratamento de dados pessoais (DPO).

Em resposta inicial quanto a este quesito, a Administração Pública municipal limitou-se, em grande medida, ao envio do contrato de implantação da solução tecnológica “LidEye” e do acordo de confidencialidade firmado entre as partes, nos quais constavam cláusulas genéricas relativas à proteção de dados e à confidencialidade.

Entre os dispositivos apresentados, destacam-se as previsões segundo as quais “a EMPREL e a SELECIONADA se comprometem a cumprir integralmente a Lei Geral de Proteção de Dados Pessoais”, bem como disposições referentes à confidencialidade, ao compartilhamento restrito de dados e à obrigação de descarte das informações ao término contratual.

A Administração também afirmou que “por não haver utilização do recurso de reconhecimento facial, declaramos a inexistência de Relatórios de Impacto à Proteção de Dados (RIPD) ou estudos de viés étnico-racial e de gênero vinculados especificamente ao Projeto LidEye”. Acrescentou-se, ainda, que os riscos decorrentes da experimentação estariam “resguardados por Termo de Confidencialidade firmado com a empresa parceira”, além do acompanhamento contínuo realizado pelo Centro de Operações do Recife (COP).

Entretanto, a resposta mostrou-se insuficiente diante da amplitude das informações requeridas. No que se refere ao enquadramento jurídico do tratamento de dados, as cláusulas contratuais apresentadas revelaram-se genéricas, sem adentrar nas especificidades constantes nos pedidos formulados.

Embora mencionem a observância da LGPD e deveres de confidencialidade, não especificam as bases legais utilizadas, os critérios de compartilhamento de dados, os mecanismos de governança, as medidas de accountability, os procedimentos de auditoria ou a delimitação precisa das responsabilidades atribuídas a cada agente envolvido. Tal omissão adquire especial relevância em razão da natureza experimental do projeto e do potencial impacto do tratamento de dados pessoais em contextos de vigilância urbana.

Diante dessas insuficiências, foi interposto primeiro recurso administrativo. Nesse recurso, sustentou-se que a ausência de reconhecimento facial não afasta, por si só, a necessidade de elaboração de RIPD, especialmente em cenários que envolvem analíticos de vídeo e tecnologias de monitoramento de espaços públicos. Argumentou-se, ainda, que cláusulas de confidencialidade não substituem os instrumentos de governança exigidos pela legislação de proteção de dados. Também se apontou a ausência de informações acerca de políticas de retenção e descarte, classificação da informação, plano de resposta a incidentes, segurança da informação e identificação formal do encarregado de dados pessoais.

Após a interposição do recurso, a Prefeitura apresentou nova resposta, reconhecendo que a solução LidEye foi aprovada “prevendo a integração direta com o Centro de Operações do Recife (COP)”, o qual atuaria como “nó centralizador” das operações envolvendo Guarda Municipal e Defesa Civil. Apesar da menção à Ata de Reunião no 03/2024, contudo, não foi concedido acesso ao documento solicitado. Quanto aos registros de acesso, informou-se que “o controle de acessos foi realizado por meio da plataforma Monuv, com trilhas de auditoria (logs) que registram cada visualização ou extração de imagem”.

O fornecimento desses registros, porém, foi negado sob fundamento genérico de proteção das estratégias de monitoramento e segurança pública. A negativa não apresentou justificativa específica quanto à impossibilidade de disponibilização parcial ou anonimizada das informações, hipótese compatível com os princípios da LAI e da própria lei de proteção de dados pessoais.

A segunda resposta também confirmou a expansão do projeto para utilização em grandes eventos, especificamente o Réveillon 2025 e o Carnaval 2025, além de ações de segurança patrimonial. Segundo a Administração, os planos operacionais teriam seguido “as diretrizes de segurança da Secretaria de Ordem Pública”, enquanto os relatórios de validação estariam “em fase de consolidação técnica pelo Conselho Gestor e CCRL”.

Ainda assim, não foram disponibilizados os documentos efetivamente requeridos, como escopo operacional, métricas de avaliação, critérios utilizados e relatórios produzidos durante a experimentação. Também permaneceu inacessível a Ata de Reunião no 01/2025 mencionada na resposta.

No campo da governança de dados, a Prefeitura passou a indicar que o “Controlador” seria a LidEye “em corresponsabilidade com a Prefeitura do Recife”, por intermédio do Conselho Gestor do EITA Labs, do CCRL e de especialistas técnicos responsáveis pela definição das finalidades e locais de teste. A empresa LidEye foi identificada como “Operador”, incumbida da coleta, do processamento em nuvem por meio da plataforma Monuv e da manutenção dos dados técnicos necessários à experimentação. Informou-se, ainda, que o encarregado de dados da EMPREL atuaria como ponto de contato para questões relacionadas ao projeto.

Apesar desse avanço parcial, permaneceram relevantes lacunas informacionais. Não houve envio de política de privacidade, política de retenção e descarte, classificação da informação, plano de resposta a incidentes ou plano de segurança da informação. Ademais, a justificativa apresentada para afastar a necessidade de RIPD mostrou-se juridicamente inadequada.

A Administração afirmou que “a obrigação de elaborar o Relatório de Impacto à Proteção de Dados (RIPD) vincula-se ao tratamento efetivo de dados biométricos”, sustentando que a mera capacidade técnica do hardware não configuraria hipótese apta a ensejar o relatório. Todavia, essa interpretação não encontra respaldo na LGPD.

Além disso, o plano de desmobilização menciona expressamente funcionalidades de “biometria facial”, além de monitoramento contínuo, analíticos avançados e integração operacional com sistemas de vigilância urbana. Ainda que a Administração sustente não haver “reconhecimento facial” em sentido estrito, a adoção de tecnologias de biometria facial já pressupõe tratamento de dados biométricos, considerados dados pessoais sensíveis pela LGPD, o que demanda elevado grau de cautela, transparência e avaliação de riscos.

Além disso, a inexistência de RIPD e de estudos sobre vieses não se justifica apenas pela negativa formal de uso de reconhecimento facial. Sistemas de videomonitoramento inteligente com analíticos automatizados, especialmente aqueles voltados à identificação de comportamentos, detecção de anomalias, classificação de indivíduos ou análise biométrica, podem produzir impactos significativos sobre direitos fundamentais, privacidade, liberdade de circulação e não discriminação, independentemente da nomenclatura adotada pela Administração.

Assim, a própria existência de operações de tratamento potencialmente aptas a produzir riscos relevantes aos titulares, especialmente em contextos de vigilância urbana,

monitoramento comportamental e coleta massiva de imagens em espaços públicos, como ocorre no presente caso, já justificaria a elaboração de Relatório de Impacto à Proteção de Dados (RIPD).

O art. 5º, inciso XVII, da Lei nº 13.709/2018 define o relatório de impacto como a documentação referente às operações de tratamento de dados pessoais capazes de gerar riscos às liberdades civis e aos direitos fundamentais dos titulares. Nesse contexto, a ausência de reconhecimento facial em sentido estrito não afasta, por si só, a necessidade de avaliação dos riscos decorrentes da utilização de sistemas de videomonitoramento inteligente, sobretudo quando há menção expressa a funcionalidades de biometria facial, analíticos automatizados e monitoramento contínuo em ambiente urbano.

Embora o ambiente de sandbox regulatório pressuponha maior flexibilidade para testes e experimentações tecnológicas, essa característica não autoriza a negligência de mecanismos mínimos de governança, transparência e proteção de direitos fundamentais.

Em razão da persistência dessas omissões, foi interposto segundo recurso administrativo, no qual se reiterou que a resposta permanecia parcial e insuficiente. Sustentou-se ainda que, embora a integração com órgãos públicos tenha sido confirmada por meio do COP, os documentos institucionais mencionados continuavam inacessíveis.

Da mesma forma, contestou-se a negativa de acesso aos logs de auditoria, especialmente diante da possibilidade de fornecimento anonimizado ou parcial. Também se requereu a definição de prazo para disponibilização dos relatórios relativos ao uso do sistema no Réveillon e no Carnaval, além da apresentação das políticas de governança de dados e de justificativa técnica robusta para a inexistência de RIPD.

Por fim, a última devolutiva da Administração limitou-se a uma resposta genérica, sem enfrentar de forma objetiva as questões suscitadas. Quanto ao acesso aos documentos solicitados, informou-se que todos os acessos aos documentos anteriormente citados como restritos foram devidamente liberados, acrescentando que se colocaram à disposição para facilitar a resolução de problemas técnicos.

Na Ata da Reunião Extraordinária no 03/2024 do Conselho Gestor do Living Labs Recife, cujo acesso foi liberado posteriormente, registrou-se a aprovação da solução LidEye para implantação e testes no âmbito do EITA Labs. A proposta foi apresentada como uma “solução de cidade inteligente com inteligência artificial embarcada”, integrada ao Centro de Operações do Recife (COP), prevendo a instalação de 100 totens com múltiplas câmeras para experimentação em ambiente urbano real. Durante a discussão, o Conselho questionou a comunicação prévia à Secretaria de Segurança Cidadã e deliberou pela formalização do envolvimento dos órgãos competentes. Também foi debatida a possibilidade de realização dos testes fora da área do Porto Digital, sendo

definida a instalação prioritária dos equipamentos nos bairros de Boa Viagem e Pina, ampliando o projeto. Ao final, a implantação da solução foi aprovada por unanimidade, com autorização temporária de uso de espaços públicos e integração operacional com os órgãos envolvidos, especialmente o COP.

Já em relação a ata da reunião extraordinária sobre o Contrato no 01/2025, foi deliberada a ampliação e realocação dos pontos de monitoramento da solução LidEye para apoiar ações de segurança patrimonial e grandes eventos, especialmente o Carnaval 2025. Entre as decisões tomadas, aprovou-se a transferência parcial de câmeras utilizadas no Réveillon Recife 2025 para o centro da cidade, bem como a instalação de novos pontos de monitoramento indicados pela Secretaria de Ordem Pública e Segurança.

A ata também determinou o acompanhamento da instalação dos equipamentos conforme o plano de trabalho vinculado ao Contrato no 035/2024 e à aprovação anterior do Conselho Gestor do EITA Labs. Além disso, foi deliberado que o COP e o CCRLl elaborariam um relatório circunstanciado sobre a experimentação realizada durante o Réveillon e o Carnaval, com o objetivo de avaliar e validar a experiência da solução tecnológica.

No que se refere ao relatório acerca do desfecho da experimentação do projeto LidEye, a Administração limitou-se a informar que “a equipe técnica está finalizando o Relatório ISES (Índice de Sucesso e Efetividade da Solução)”, acrescentando que o documento ainda será submetido à homologação do Conselho do EITA! Labs na próxima reunião ordinária. Dessa forma, não foram apresentados elementos concretos sobre os resultados efetivos da experimentação, os critérios de avaliação empregados ou as conclusões já alcançadas no âmbito do projeto.

IJ. Controle, monitoramento e avaliação de desempenho operacional

O conjunto de perguntas IJ teve como objetivo apurar quais mecanismos concretos de fiscalização, avaliação de desempenho, controle operacional e accountability foram efetivamente aplicados à iniciativa LidEye durante sua implementação e operação no âmbito da Prefeitura do Recife. Questionou-se a existência de supervisão institucional pela Emprel, CCRLl e Conselho Gestor, além de métricas, relatórios de avaliação, indicadores de sucesso, registros de falsos positivos, revisão humana e canais de contestação sobre os totens de monitoramento. Por fim, procurou-se identificar se a implementação da tecnologia foi acompanhada de mecanismos de transparência e participação social, como consultas e audiências públicas com a sociedade civil.

Foram solicitadas informações e documentos relacionados aos: a) mecanismos de fiscalização, avaliação, monitoramento operacional e controle institucional do projeto LidEye, incluindo registros de supervisão realizados pela Emprel, pelo CCRLl e pelo Conselho Gestor; b) relatórios de Índice de Sucesso (ISES) ou avaliações equivalentes; c)

métricas utilizadas para aferição de desempenho e metodologia adotada para avaliação dos resultados; d) estatísticas anonimizadas sobre abordagens, detenções e encaminhamentos decorrentes dos alertas antes da adoção de medidas operacionais; e) registros de falsos positivos, incidentes, reclamações e procedimentos de correção; f) documentos relativos à existência de canais de contestação; g) além de informações sobre eventual realização de consultas públicas, audiências ou mecanismos de participação social relacionados à implementação e operação da tecnologia.

Em resposta inicial, a Prefeitura limitou-se, basicamente, a indicar cláusulas genéricas do CONTRATO AJU no 035/2024 relacionadas à fiscalização do projeto pela Emprel, Conselho Gestor e CCRL, bem como mencionar que o EITA! Labs adota parâmetros próprios para a avaliação ISES durante a fase experimental da iniciativa. Contudo, não foram apresentados relatórios, pareceres, atas, métricas, estatísticas operacionais ou quaisquer documentos concretos relacionados à fiscalização efetiva do LidEye, à avaliação de desempenho da solução, à ocorrência de falsos positivos, à revisão humana dos alertas emitidos pelos totens ou à existência de mecanismos de contestação e participação social. A resposta também não esclareceu objetivamente se essas informações e documentos existiam ou não, deixando sem manifestação expressa diversos pontos centrais do pedido e sem justificativa específica para a ausência das informações solicitadas.

No primeiro recurso do pedido IJ, sustentou-se que a resposta permanecia materialmente insuficiente por limitar-se a referências genéricas ao contrato e omitir os itens da consulta inicial. Apontou-se que a Administração não esclareceu se houve fiscalização efetiva pela Emprel, CCRL e Conselho Gestor, deixando de apresentar relatórios, atas ou pareceres desse acompanhamento. Destacou-se também a ausência de manifestação sobre o relatório ISES, métricas de desempenho, estatísticas operacionais, validação humana, falsos positivos, canais de contestação e participação social. Além disso, questionou-se a falta de declaração formal de inexistência dos dados ou de justificativa para eventual restrição de acesso, requerendo a complementação integral nos termos da LAI.

Após o primeiro recurso, a Prefeitura apresentou esclarecimentos adicionais e novos documentos, como atas do Conselho Gestor do Recife Living Labs e o Plano de Mobilização e Desmobilização do projeto LidEye. A Administração afirmou que houve fiscalização por instâncias como Emprel/DIAG, CCRL e COP, e informou que o relatório ISES estava em fase de homologação. Também declarou inexistirem métricas operacionais, estatísticas de abordagens e registros de reclamações devido à natureza experimental do projeto, confirmando a validação humana de alertas no COP e a ausência de audiências públicas. Contudo, permaneceram lacunas sobre a documentação integral de fiscalização, métricas utilizadas, critérios metodológicos, falsos alertas e registros operacionais. Diante disso, o segundo recurso reiterou a necessidade de acesso integral aos documentos citados e de esclarecimentos objetivos sobre a fiscalização, avaliação e controle do projeto.

Mesmo após o recurso final, permaneceram sem esclarecimento adequado informações centrais sobre a fiscalização efetiva do projeto LidEye, critérios de desempenho, métricas, validação humana, registros de falsos positivos, incidentes, canais de contestação e participação social. A Prefeitura do Recife tampouco apresentou relatórios e pareceres técnicos que demonstrassem a supervisão da Emprel, do Conselho Gestor e do CCRL, limitando-se a referências genéricas de governança. Embora tenha citado a futura homologação do Relatório ISES, não forneceu dados sobre seu conteúdo, metodologia ou cronograma. Juridicamente, a resposta permaneceu frágil ao omitir a declaração formal de inexistência de vários documentos e ao não fundamentar sua não disponibilização, violando a LAI. Por fim, a manifestação não analisou individualmente o recurso, reproduzindo argumentos anteriores de forma protocolar, defensiva e sem adaptação substancial à demanda.

Ao fim, concluímos que a qualidade da resposta administrativa mostrou-se limitada e predominantemente protocolar, marcada por elevado grau de generalidade e baixa capacidade de esclarecimento efetivo dos aspectos operacionais, metodológicos e institucionais relacionados ao projeto LidEye. Embora a Prefeitura do Recife tenha apresentado complementações pontuais ao longo do procedimento recursal, as manifestações não ampliaram substancialmente a transparência sobre os mecanismos concretos de fiscalização, avaliação de desempenho, controle de riscos e *accountability* aplicáveis à tecnologia, restringindo-se majoritariamente ao cumprimento formal da obrigação de responder aos pedidos formulados.

K. Governança ética da inteligência artificial e salvaguardas de direitos

Os pedidos enviados na consulta K tiveram como objetivo apurar se a Prefeitura do Recife possuía mecanismos formais de governança algorítmica, supervisão ética e salvaguardas institucionais relacionados ao uso de sistemas de inteligência artificial, monitoramento automatizado e biometria facial no âmbito do sistema LidEye e do programa EITA! Labs. O pedido de acesso à informação fez questionamentos, especialmente, quanto à existência de normas, diretrizes, *frameworks* éticos, avaliações de impacto, mecanismos de transparência, auditoria, mitigação de vieses discriminatórios e estudos sobre proporcionalidade e alternativas menos intrusivas para políticas de segurança urbana e vigilância em espaços públicos.

Foram solicitadas informações e documentos relacionados à: a) governança, regulação e controle do uso de sistema de inteligência artificial e monitoramento automatizado pela Prefeitura, incluindo leis, normas e diretrizes utilizadas como balizas para a adoção dessas tecnologias; b) *frameworks* éticos, protocolos institucionais e políticas de governança aplicáveis ao programa EITA Labs e ao sistema LidEye; c) relatórios, avaliações e estudos de impacto algorítmico, proteção de dados e direitos fundamentais;

d) estudos técnicos sobre vieses e impactos discriminatórios; e) documentos relativos a mecanismos de auditoria, transparência, *accountability* e explicabilidade de sistemas algorítmicos; f) além de estudos ou notas técnicas que comparassem o uso de reconhecimento facial e tecnologias equivalentes com alternativas menos intrusivas de segurança urbana.

Em resposta inicial, a Prefeitura limitou-se a indicar normas do *sandbox* regulatório e a enviar documentos contratuais do projeto LidEye, como termos de confidencialidade e implantação. A Administração negou a existência de Relatórios de Impacto à Proteção de Dados (RIPD) ou estudos de viés sobre reconhecimento facial, alegando que a funcionalidade não estava em uso no decorrer do projeto. Afirmou, genericamente, que os riscos são resguardados pelo termo de confidencialidade e pelo monitoramento do Centro de Operações do Recife (COP). Contudo, não foram apresentados *frameworks* éticos, políticas de governança algorítmica, auditoria, transparência ou estudos de impacto sobre outros sistemas de IA. O município também pecou pela ausência de avaliações de direitos fundamentais e de alternativas menos intrusivas de segurança, deixando de esclarecer expressamente a existência de vários documentos solicitados.

No primeiro recurso administrativo, sustentou-se que a resposta foi parcial e insuficiente por não apresentar os documentos solicitados nem esclarecer adequadamente a existência das informações. Apontou-se que a Administração restringiu indevidamente o escopo ao reconhecimento facial, omitindo outros sistemas de IA e monitoramentos automatizados do projeto LidEye. Destacou-se também a ausência de *frameworks* de governança, avaliações de impacto algorítmico e de direitos fundamentais, auditoria, transparência, estudos de viés e análises de alternativas menos intrusivas. Por fim, questionou-se a contradição entre a alegada falta de estudos de impacto e a afirmação de que os riscos estariam resguardados, sem a devida documentação ou fundamentação formal de restrição baseada na LAI.

Após o primeiro recurso, a Prefeitura apresentou esclarecimentos adicionais, indicando normas gerais aplicáveis – como a LGPD, o decreto do *sandbox* regulatório e a estratégia municipal de IA, esta última implantada após o encerramento do projeto LidEye – e confirmando a ausência de regulação específica sobre reconhecimento facial e IA. A Administração declarou não possuir *framework* ético ou checklist para IA, sustentando que a governança ocorreria de forma colegiada pelo CCRL. Além de reiterar a inexistência de RIPD, estudos de viés e avaliações de impacto sobre reconhecimento facial no projeto LidEye, o município mencionou genericamente auditorias internas, *dashboards* e o uso da metodologia de avaliação ISES. Contudo, não apresentou os documentos técnicos correspondentes nem esclareceu a existência de avaliações sobre outros analíticos de vídeo e monitoramento automatizado.

Diante da persistência dessas lacunas, o segundo recurso administrativo sustentou

que as respostas permaneciam materialmente insuficientes, reiterando a necessidade de fornecimento integral dos documentos solicitados, de esclarecimentos sobre diretrizes práticas de governança de IA, avaliações de impacto relativas a outros sistemas algorítmicos e disponibilização efetiva dos mecanismos de auditoria mencionados, além de apontar a restrição de acesso à Ata de Reunião no 03/2024 pela Gestão Municipal.

Apesar dos recursos, permaneceram obscuros aspectos centrais de governança algorítmica, avaliações de impacto, auditoria, transparência e supervisão ética do LidEye. Na última resposta, a Prefeitura seguiu sem informar objetivamente a existência de protocolos internos, critérios de governança e mecanismos de *accountability* para IA e monitoramento automatizado. Além disso, limitou-se a referências genéricas de metodologias e relatórios sem disponibilizar o conteúdo. A principal fragilidade jurídica e técnica consistiu em restringir a discussão ao reconhecimento facial para afastar a necessidade de RIPD, estudos de viés e avaliações de impacto, ignorando o escopo amplo da demanda sobre outros analíticos de vídeo potencialmente lesivos a direitos fundamentais. Por fim, a última resposta não analisou individualmente os argumentos recursais, repetindo textos anteriores de forma protocolar, defensiva e sem adaptação substancial.

De modo geral, a qualidade das respostas administrativas mostrou-se limitada por elevado grau de generalidade, insuficiência material e baixa capacidade de esclarecimento. Embora tenha trazido referências a normas, instâncias colegiadas e mecanismos de acompanhamento, a Prefeitura do Recife não apresentou documentação técnica ou critérios objetivos de governança capazes de ampliar a transparência sobre o funcionamento e o controle do projeto LidEye. A resposta final assumiu caráter protocolar e defensivo, concentrando-se no cumprimento formal da obrigação de responder aos recursos em detrimento do efetivo enfrentamento das questões de governança algorítmica, proteção de dados, transparência e salvaguardas aplicáveis ao monitoramento automatizado.



CONCLUSÃO COM ATUALIZAÇÕES

Na data de 29 de julho de 2026, após o fechamento do relatório, a Prefeitura do Recife publicou o Relatório ISES referente à experimentação da solução LidEye no âmbito do EITA! Labs, documento cuja existência havia sido reiteradamente informada ao longo da tramitação dos pedidos de acesso à informação, mas que permaneceu indisponível durante toda a fase de coleta de dados desta pesquisa.

Sua publicação representa um avanço em relação ao cenário descrito neste relatório, ao tornar pública a avaliação final da experimentação e reconhecer que a solução não atingiu o desempenho mínimo exigido para validação no sandbox regulatório, obtendo nota final de 6,55 e sendo reprovada em razão de limitações técnicas, elevado custo operacional, dependência de fatores externos, impacto limitado e baixo diferencial inovador.

Não obstante, a divulgação do relatório não altera substancialmente as conclusões alcançadas nesta pesquisa. Embora apresente algumas informações anteriormente indisponíveis, o documento permanece predominantemente descritivo e carece de elementos metodológicos suficientes para permitir a verificação independente de suas conclusões.

Os chamados “resultados operacionais” são apresentados apenas como estimativas, sem indicação da metodologia de cálculo, da base empírica utilizada, do período de referência ou dos registros administrativos que lhes dão suporte. Do mesmo modo, o relatório não disponibiliza métricas individualizadas de efetividade, estatísticas de falsos positivos, critérios de validação dos analíticos, avaliações de impacto em proteção de dados ou direitos fundamentais, nem esclarecimentos adicionais sobre governança algorítmica, auditoria, transparência ou accountability.

Chama atenção, ainda, que as recomendações decorrentes da experimentação concentram-se exclusivamente no aprimoramento técnico e operacional da solução - como conectividade-



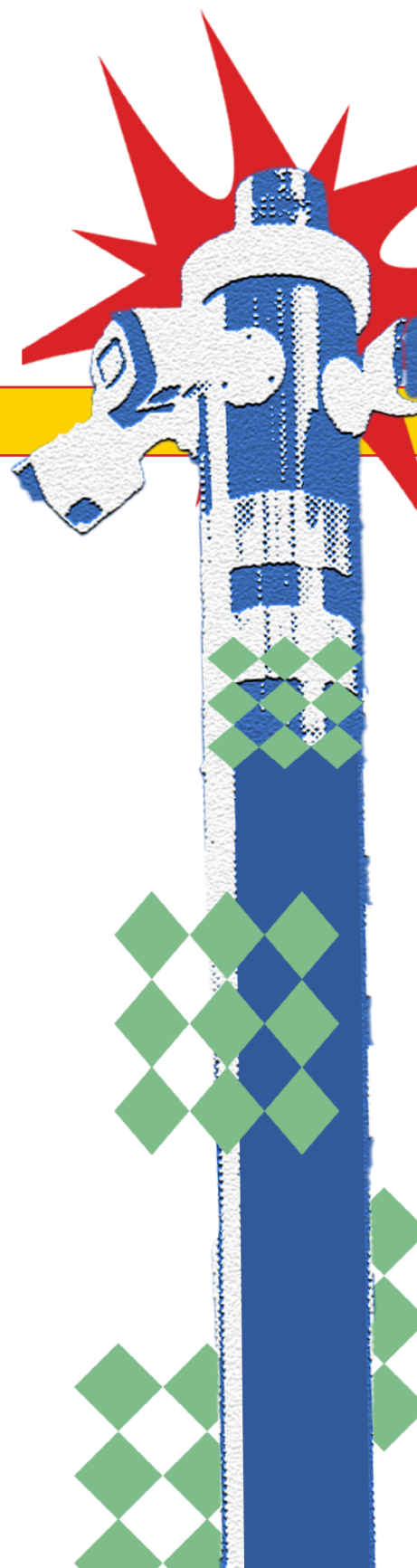
de, manutenção, integração tecnológica e expansão futura - sem qualquer recomendação relacionada à privacidade, proteção de dados pessoais, mitigação de riscos aos direitos fundamentais, participação social ou mecanismos de supervisão e controle, apesar de esses temas terem constituído um dos principais objetos dos pedidos de acesso à informação e desta pesquisa.

Assim, embora a publicação do ISES represente um incremento relevante de transparência, ela não supre as lacunas documentais e informacionais identificadas ao longo deste relatório nem modifica suas conclusões centrais acerca das fragilidades de governança e prestação de contas do projeto LidEye.

RECOMENDAÇÕES MULTISSETORIAIS PROPOSTAS

As análises desenvolvidas ao longo deste relatório evidenciam que os desafios relacionados à implementação de sistemas de videomonitoramento inteligente transcendem questões estritamente tecnológicas, envolvendo aspectos de governança pública, transparência, proteção de dados, participação social, controle democrático e respeito aos direitos humanos.

Nesse contexto, as recomendações apresentadas a seguir foram estruturadas sob uma perspectiva multissetorial, reconhecendo que o fortalecimento da governança dessas tecnologias depende da atuação coordenada do Poder Executivo, Poder Legislativo, Poder Judiciário - segmentados, ante suas competências como "setor governamental" -, empresas, sociedade civil e academia.





Poder Executivo

- Instituir um marco regulatório municipal para sistemas de videomonitoramento inteligente, disciplinando requisitos mínimos para aquisição, experimentação e operação de tecnologias de IA, biometria e reconhecimento facial.

- Tornar obrigatória a realização de avaliações de impacto em direitos fundamentais e proteção de dados (AIDP/RIPD) antes da implantação ou expansão de qualquer sistema de vigilância algorítmica, assegurando publicidade dos relatórios e consulta pública prévia.

- Criar uma Política Municipal de Governança Algorítmica, estabelecendo princípios de legalidade, necessidade, proporcionalidade, explicabilidade, supervisão humana, mitigação de vieses, accountability e gestão de riscos.

- Institucionalizar mecanismos de participação pública significativa, garantindo consultas públicas desde a fase de planejamento, audiências, publicação de versões preliminares dos projetos e devolutivas fundamentadas às contribuições recebidas, em consonância com as recomendações da OCDE.

- Implementar transparência ativa permanente, mediante portal público contendo contratos, avaliações de impacto, relatórios de desempenho, indicadores, localização dos equipamentos, fornecedores, funcionalidades empregadas, critérios de funcionamento e documentação produzida durante experimentações.

- Criar mecanismos permanentes de auditoria independente e avaliação periódica, incluindo revisão da efetividade da política pública, análise de custo-benefício, impactos discriminatórios, falsos positivos e possibilidade de suspensão ou encerramento de tecnologias que não demonstrem benefícios proporcionais.



Recomendações específicas para o EITA! Labs (Prefeitura do Recife)

- Instituir um protocolo específico para tecnologias de alto risco, estabelecendo requisitos diferenciados para projetos que envolvam inteligência artificial, biometria, reconhecimento facial e outras tecnologias de vigilância, em razão do seu potencial impacto sobre direitos fundamentais.

- Tornar obrigatória a realização e publicação de avaliações prévias de impacto, incluindo Relatório de Impacto à Proteção de Dados (RIPD), avaliação de impacto em direitos humanos, análise de riscos algorítmicos e justificativa de necessidade, proporcionalidade e subsidiariedade antes da aprovação de qualquer projeto.

- Incorporar mecanismos de participação pública significativa ao ciclo de experimentação, prevendo consultas públicas, audiências e divulgação prévia das soluções tecnológicas de maior impacto, com respostas fundamentadas às contribuições apresentadas pela sociedade.

- Reestruturar a composição do Conselho Gestor e das instâncias decisórias, assegurando participação de representantes da sociedade civil, academia, órgãos de controle, especialistas independentes e organizações de direitos humanos, fortalecendo a governança multisetorial do programa.

- Fortalecer a transparência ativa do programa, mediante a criação de um portal público contendo editais, projetos aprovados, pareceres técnicos, atas, contratos, avaliações de impacto, indicadores de desempenho, critérios de seleção e relatórios finais de cada experimentação.





- Estabelecer critérios objetivos para expansão, alteração ou encerramento dos projetos, exigindo motivação técnica, nova deliberação formal, publicidade das decisões e demonstração de que as alterações permanecem compatíveis com os objetivos originalmente autorizados para o sandbox.

- Instituir uma Política de Governança de Inteligência Artificial do EITA! Labs, contemplando princípios de supervisão humana, mitigação de vieses, explicabilidade, gestão de riscos, accountability, auditoria e proteção de dados pessoais.

- Restringir o uso de cláusulas de confidencialidade, vedando sua utilização para limitar o acesso a documentos relacionados à governança pública, avaliações de impacto, critérios decisórios, medidas de mitigação de riscos e demais informações de interesse coletivo.

- Padronizar a avaliação dos projetos experimentais, estabelecendo indicadores mínimos de desempenho, efetividade, impactos sobre direitos fundamentais, ocorrência de falsos positivos, custo-benefício e resultados obtidos durante a experimentação.

- Submeter tecnologias de vigilância inteligente à auditoria técnica independente, realizada periodicamente por instituições externas com capacidade técnica, assegurando avaliação imparcial sobre desempenho, conformidade jurídica, proteção de dados e impactos sociais.

- Instituir mecanismos permanentes de prestação de contas e controle social, com publicação periódica de relatórios de transparência, realização de reuniões públicas de acompanhamento e disponibilização de canais específicos para denúncias, reclamações e exercício dos direitos dos titulares de dados.

- Definir critérios claros para a transição entre experimentação e implementação permanente, condicionando a incorporação definitiva de qualquer tecnologia à demonstração pública de sua efetividade, proporcionalidade, conformidade com a LGPD, respeito aos direitos fundamentais e validação por processo decisório transparente e participativo.



Poder Legislativo

- Aprovar legislação específica sobre videomonitoramento inteligente e reconhecimento facial, estabelecendo limites materiais, finalidades legítimas e salvaguardas para direitos fundamentais.
- Exigir autorização legislativa para programas estruturantes de vigilância algorítmica, especialmente aqueles envolvendo biometria, IA ou monitoramento contínuo de espaços públicos.
- Instituir obrigações legais de transparência algorítmica, impondo publicidade mínima sobre modelos utilizados, finalidades, métricas de desempenho, avaliações de impacto e auditorias.
- Criar mecanismos permanentes de fiscalização parlamentar, mediante comissões temáticas ou relatórios periódicos obrigatórios apresentados pelo Executivo.
- Condicionar a utilização de recursos públicos à demonstração de efetividade baseada em evidências, vedando investimentos em tecnologias cuja eficácia permaneça não comprovada.
- Assegurar participação social institucionalizada na elaboração das normas, envolvendo sociedade civil, academia, setor privado, grupos vulnerabilizados e autoridades independentes.



Poder Judiciário

- Consolidar parâmetros jurisprudenciais para o controle judicial de sistemas algorítmicos utilizados pelo Estado, especialmente quanto aos princípios da proporcionalidade, necessidade e legalidade.
- Estimular a produção antecipada de provas técnicas, permitindo perícias independentes sobre funcionamento, acurácia e riscos dos sistemas de IA empregados pelo Poder Público.
- Adotar interpretação ampliativa quanto ao dever de elaboração de Relatórios de Impacto, reconhecendo que analíticos de vídeo e monitoramento inteligente também podem justificar avaliações prévias de risco.
- Fortalecer o controle sobre alegações genéricas de sigilo comercial, exigindo demonstração concreta da imprescindibilidade da restrição ao acesso à informação.
- Incentivar soluções estruturantes, privilegiando decisões que determinem aperfeiçoamentos institucionais de transparência e governança, para além da solução de casos individuais.
- Promover capacitação continuada de magistrados e servidores em inteligência artificial, proteção de dados, direitos humanos e discriminação algorítmica.



Empresas

- Adotar políticas de Direitos Humanos por Design e Privacy by Design, incorporando salvaguardas desde a concepção das soluções tecnológicas.
- Realizar avaliações independentes de impacto em direitos humanos e riscos algorítmicos, disponibilizando versões públicas sempre que atuem junto ao Poder Público.
- Fornecer documentação técnica suficiente para auditorias públicas, preservando segredos industriais apenas naquilo que seja estritamente necessário.
- Mensurar e divulgar indicadores de desempenho, incluindo taxas de erro, falsos positivos, vieses, limitações conhecidas e métricas de efetividade.
- Estabelecer mecanismos acessíveis de contestação e reparação, permitindo que pessoas afetadas por decisões automatizadas possam exercer seus direitos.
- Comprometer-se contratualmente com padrões internacionais de IA responsável, observando princípios de não discriminação, transparência, explicabilidade, supervisão humana e prestação de contas.



Sociedade Civil

- Fortalecer mecanismos independentes de monitoramento cívico sobre tecnologias de vigilância e inteligência artificial empregadas pelo Poder Público.
- Ampliar o uso estratégico da Lei de Acesso à Informação, promovendo auditorias sociais permanentes sobre políticas tecnológicas.
- Produzir avaliações independentes dos impactos sociais, especialmente sobre populações historicamente vulnerabilizadas.
- Estimular processos deliberativos multissetoriais, aproximando organizações sociais, comunidades locais, setor público e especialistas na construção das políticas.
- Promover educação pública sobre direitos digitais, privacidade, proteção de dados e funcionamento de sistemas algorítmicos.
- Articular redes nacionais e internacionais de incidência, compartilhando metodologias, evidências e boas práticas sobre governança democrática da inteligência artificial.



Academia

- Produzir avaliações independentes de efetividade, comparando tecnologias de vigilância inteligente com alternativas menos intrusivas para segurança pública.
- Desenvolver metodologias padronizadas para auditoria algorítmica, aplicáveis a sistemas utilizados pelo setor público.
- Realizar pesquisas sobre vieses discriminatórios e impactos desiguais, considerando marcadores de raça, gênero, idade, território e vulnerabilidade social.
- Contribuir para a elaboração de padrões técnicos e regulatórios, aproximando produção científica e formulação de políticas públicas.
- Constituir observatórios permanentes de IA e vigilância urbana, produzindo indicadores, bases de dados abertas e avaliações periódicas.
- Ampliar programas de extensão e formação continuada, capacitando gestores públicos, parlamentares, operadores do direito e organizações da sociedade civil sobre governança de inteligência artificial, proteção de dados e direitos humanos.



Instituto de
Pesquisa em
Direito & Tecnologia
do Recife

 @ip.rec

 ip.rec.br

