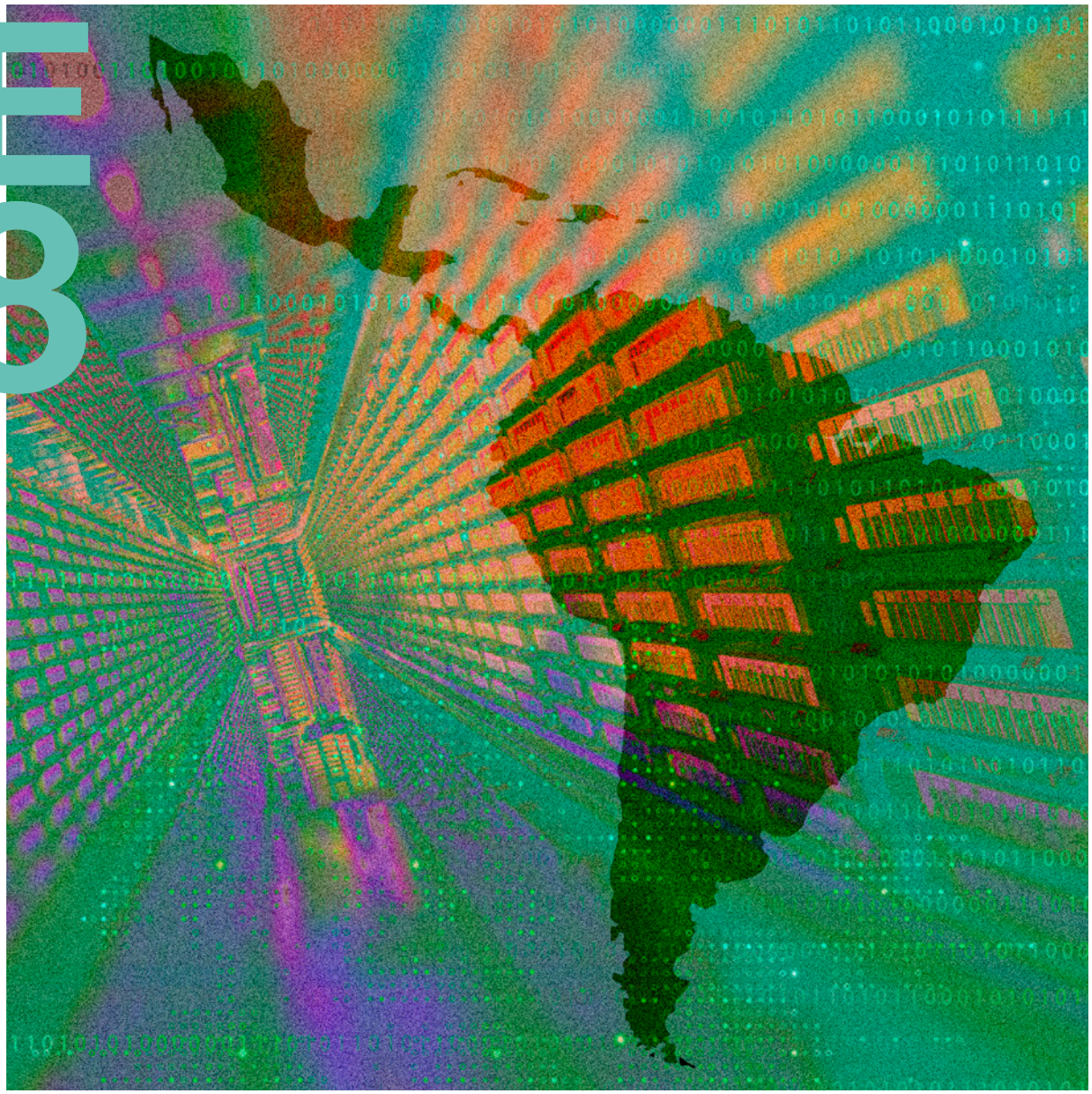
INSTITUTO IGARAPÉ
a think and do tank

AE 58

ARTIGO ESTRATÉGICO 58

NOVEMBRO DE 2022



IMPLEMENTAÇÃO DE TECNOLOGIAS DE VIGILÂNCIA NO BRASIL E NA AMÉRICA LATINA

IMPLEMENTAÇÃO DE TECNOLOGIAS DE VIGILÂNCIA NO BRASIL E NA AMÉRICA LATINA

Sumário Executivo

A chegada da pandemia no Brasil provocou um processo de digitalização forçada, levando muitos a dependerem de aplicativos de mensageria privada para manter seus negócios. Em maio de 2021, o Comitê Gestor da Internet (CGI.br) detectou 11 Tbps de tráfego de dados na rede, batendo um recorde histórico[1]. Em um momento de isolamento social e controle da crise sanitária, a digitalização tornou-se condição básica para o funcionamento da economia e da sociedade. Países como o Brasil e outros na América Latina também olharam para a tecnologia como uma auxiliadora no controle da crise sanitária. Contudo, o tecno-solucionismo no gerenciamento de uma crise não se deu isoladamente, pelo contrário, essas tecnologias de monitoramento se somam à uma infraestrutura de vigilância setorial já existente e apresentam novas tendências e riscos a liberdades e direitos em um contexto de vigilantismo já preocupante.

O problema é que, por mais que a implementação de algumas tecnologias (reconhecimento facial) e setores (segurança pública) sejam altamente noticiados, permanecemos com uma visão parcial e fragmentada das práticas de implementação de tecnologias de vigilância pelo setor público – ora focando em uma, ora focando em outra. Com isso em mente, apresentamos o relatório **Implementação de Tecnologias de Vigilância no Brasil e na América Latina**, resultado da aplicação da nossa Tipologia[2] na análise de mais de 300 casos mapeados no Brasil e em outros países da América Latina entre 2006 e 2021. O relatório apresenta as principais tendências de implementação de tecnologias de vigilância em sete setores: segurança pública, saúde, educação, economia, transportes, inteligência e eventos/turismo.

Sem monitoramento, regulação e controle essas tecnologias podem se tornar um desafio frente à proteção de dados e demais direitos no século XXI. Reconhecemos que ainda temos muito a mapear e cremos que a Tipologia poderá auxiliar outras organizações do terceiro setor, academia e setor público no processo de mapeamento de projetos, tecnologias e impactos associados à vasta adesão de soluções para o setor público.

1 Gomes, Mariana (2021) in Le Monde Diplomatique Brasil. A naturalização de sistemas e tecnologias de vigilância na pandemia. Disponível em: https://diplomatique.org.br/a-naturalizacao-de-sistemas-e-tecnologias-de-vigilancia-na-pandemia/

2 Instituto Igarapé (2022). Uma tipologia para analisar a implementação de tecnologias de vigilância pelo Estado. Disponível em: LINK

Principais Achados

- Desde 2006, o período com maior crescimento na aplicação de tecnologias de vigilância foi entre 2020 e 2021.

- Segurança pública é o setor que lidera na implementação de tecnologias de vigilância, com 76,4% dos casos publicamente reportados no Brasil e 54% dos casos em demais países da América Latina.

- Tecnologias de vigilância são majoritariamente usadas para o monitoramento do fluxo de pessoas e objetos, representando 38% dos casos no Brasil[3] e 23,5%[4] na América Latina.

- No Brasil, o videomonitoramento lidera como a principal funcionalidade (31,3% dos casos). Já nos demais países da América Latina os casos concentram-se não apenas nessa tecnologia, mas também em reconhecimento facial (12,3% dos casos).

- Tal como em segurança pública, o monitoramento de fluxos de pessoas se tornou uma função prioritária no setor de saúde (31,3%)[5] e é realizada principalmente por intermédio de aplicativos, monitoramento geoespacial e de temperatura.

- O monitoramento de fluxo de pessoas e medição de temperatura foi algo imprescindível na pandemia. Tecnologias como videomonitoramento e reconhecimento facial foram adaptadas ao novo cenário de emergência sanitária, identificando rostos com ou sem máscaras e auferindo a temperatura de passantes.

- O setor de saúde é o que mais coleta dados de diferentes naturezas no Brasil (ver gráfico 5).

- O setor de inteligência representa 2,5% dos casos mapeados no Brasil[6] e 3,2%[7] na América Latina. Apesar do baixo percentual — resultante da falta de transparência sobre aquisições no setor — a natureza intrusiva das tecnologias empregadas as tornam de igual ou de maior preocupação.

---

3 A partir de um universo de 424 funcionalidades mapeadas no setor para Brasil.

4 A partir de um universo de 81 funcionalidades mapeadas no setor para demais países da América Latina contemplados pela pesquisa.

5 A partir de um universo de 80 funcionalidades mapeadas no setor para Brasil.

6 A partir de um universo de 237 casos mapeados no Brasil.

7 A partir de um universo de 63 casos mapeados nos demais países da América Latina contemplados pela pesquisa.

Sumário

Introdução

Ao longo dos anos, as práticas de vigilância evoluíram, e proporcionaram novas formas de medir, rastrear, mapear e vigiar corpos e comportamentos. Em setores como o da segurança pública, uma variedade de novas técnicas em vigilância vem acompanhando o célere desenvolvimento tecnológico. O Centro de Segurança e Estudos da ETH Zürich relatou que o mercado de câmeras de vigilância esperava um substancial crescimento em 2021, atingindo a marca de 300.000 novas câmeras sendo instaladas todos os dias, em todo o mundo[8]. Na saúde, a propagação da pandemia serviu como potencializador na adoção de novas tecnologias de monitoramento. Essas tecnologias incluem scanners térmicos, sistemas de reconhecimento facial e programas para coletar e analisar massivas quantidades de dados digitais. Dado o cenário epidêmico, novas preocupações surgem: é necessário não somente vigiar o fluxo de pessoas, como também detectar o uso ou não de máscaras, identificar indivíduos com a temperatura acima do padrão, fazer rastreamento de contatos e monitorar áreas de risco, assim como emitir passaportes de imunização.

O vigilantismo é algo complexo, que precisa ser compreendido na sua aplicação multifacetada por diferentes setores. Mas o desafio é que não temos dados estruturados sobre práticas de implementação, o que inviabiliza um conhecimento mais contextualizado de tendências. O que se apresenta no âmbito da América Latina é um cenário fragmentado de casos diversos de implementação de tecnologias de vigilância, em diferentes setores para múltiplas finalidades. A população acompanha esses processos, em grande medida, a partir de pautas que ganham atenção nos grandes veículos de mídia. Por mais importantes que esses veículos sejam no seu exercício de informar e trazer a atenção do público a assuntos correntes, o curto ciclo de notícias, por vezes, traça uma visão imediatista dos desafios que permeiam a vigilância. Por isso, faz-se necessário aliar reportagens com o desenvolvimento de estudos que possam trazer uma maior perspectiva temporal.

Por esses motivos, o Instituto Igarapé desenvolveu uma tipologia para monitorar casos de implementação de tecnologias de vigilância[9] (ver anexo 1 para versão resumida). No presente relatório, apresentamos uma visão aplicada da tipologia na forma de um mapeamento setorial sobre o vigilantismo no Brasil e na América Latina. Esse exercício inclui um estudo aprofundado de 7 setores: economia, educação, inteligência, saúde, eventos/turismo, transporte e segurança pública. Os resultados apresentados baseiam-se em mais de 300 casos de implementação de tecnologias de vigilância levantados no Brasil[10] e em outros países na na América Latina[11] entre 2006 e 2022. Esses casos foram mapeados através de pesquisa em fontes secundárias, e, principalmente, em fontes midiáticas. Para os casos reportados no Brasil, realizamos um levantamento de fontes primárias por meio de buscas em portais de transparência e acesso à informação, como TCU[12] e portais estaduais de compras.

8 Salvo, 2021

9 Instituto Igarapé (2022). Uma tipologia para analisar a implementação de tecnologias de vigilância pelo Estado. Disponível em: LINK

10 237 casos mapeados no Brasil e 63 na América Latina.

11 Ao mencionarmos América Latina no contexto desta pesquisa, nos referimos aos seguintes países: Argentina, Colômbia, Chile, México, Uruguai, Bolívia, Equador, Peru, Venezuela, El Salvador, Honduras, Panamá e Paraguai.

12 Tribunal de Contas da União.

O presente documento está dividido em 2 partes. Na primeira seção, apresentamos um panorama geral dos casos mapeados no Brasil e demais países da América Latina: o que inclui o contexto de implementação, seus principais setores, a evolução temporal dos casos mapeados ao longo de 14 anos e os países e estados em destaque. Na segunda seção, aprofundamos o olhar sobre as principais características da vigilância em cada um dos 7 setores mapeados (as principais tecnologias, tipos de dados coletados, entre outros elementos).

Visão geral: tendências na implementação de tecnologias de vigilância

As tecnologias de vigilância, principalmente aquelas baseadas em sistemas de Inteligência Artificial (IA), já estão oficialmente presentes em 75 países do mundo[13]. A América Latina e o Brasil não fogem desse contexto. Nesta seção, apresentamos um panorama dos principais dados de nosso mapeamento, o qual inclui uma visão geral e setorial da implementação de tecnologias de vigilância na região, o cenário de desenvolvedores que apoiam esses projetos, bem como uma perspectiva dos principais tipos de dados coletados por essas tecnologias.

Um panorama da América Latina e do Brasil

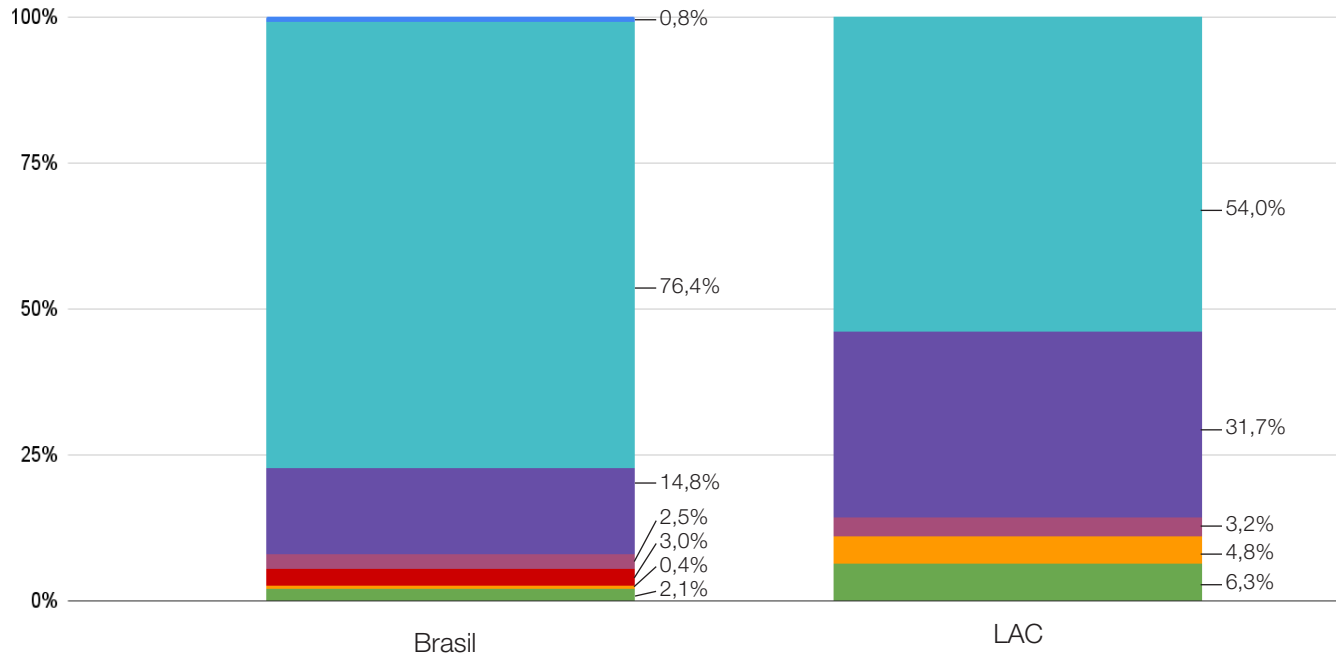
A América Latina é uma região complexa com diferentes níveis de digitalização, taxas de acesso à Internet[14], persistentes desafios relacionados à violência urbana e grandes disparidades socioeconômicas. A tecnologia é apresentada ao Estado como força motriz para o desenvolvimento nacional e transformação digital. Mais do que isso, e especialmente em países em desenvolvimento como os da região, algumas dessas tecnologias são apresentadas como soluções para problemas estruturais de falta de pessoal e ineficiência das atividades de policiamento, mas acabam ampliando não só a vigilância, como as tendências socioeconômicas e raciais desses processos.

Nem só de promessas ou críticas vivem essas tecnologias. Os setores de segurança pública e de saúde concentram grande parte dos projetos de implementação de tecnologias de vigilância (Gráfico 1) – **com 76% dos casos do Brasil e 54% na América Latina concentrando-se em segurança pública, seguidos de 32% dos casos no setor de saúde.**

13 Dados de 2018 em Feldstein, 2019.

14 OECD (2020). Latin American Economic Outlook 2020 : Digital Transformation for Building Back Better. Disponível em: https://www.oecd-ilibrary.org/sites/e7a00fd6-en/index.html?itemId=/content/component/e7a00fd6-en

Gráfico 1 e Tabela 1: Implementação de tecnologias de vigilância por setor (Brasil e América Latina)



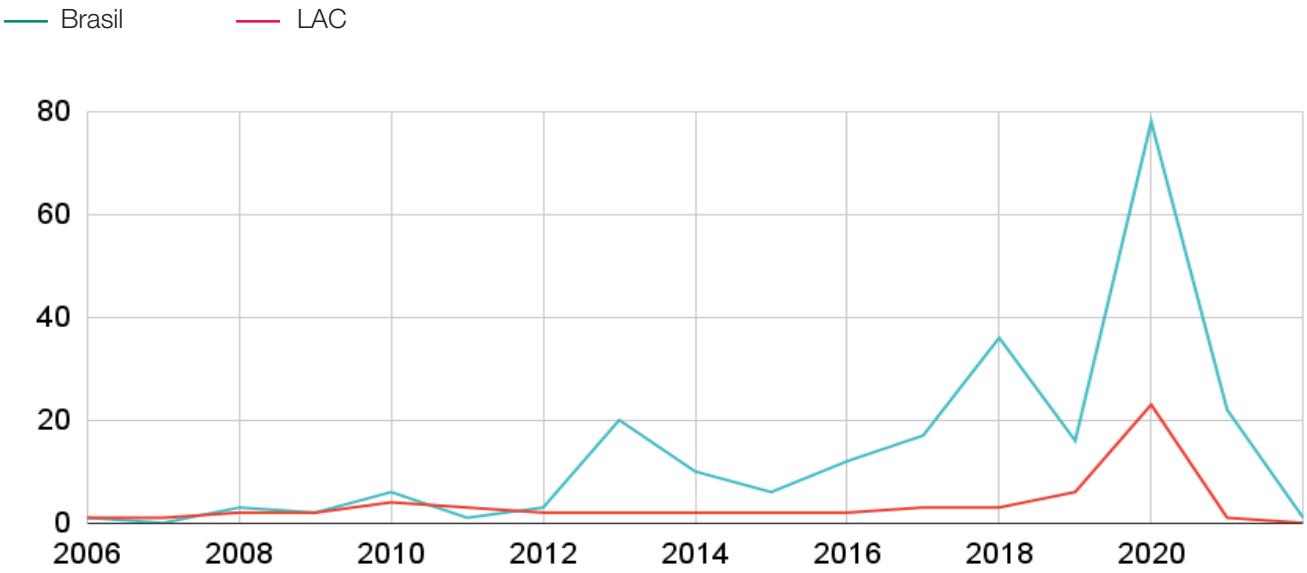
	Setor	Brasil	LAC	Total
	Economia	5	4	9
	Educação	1	3	4
	Eventos/Turismo	7	0	7
	Inteligência	6	2	8
	Saúde	35	20	55
	Segurança Pública	181	34	215
	Transporte	2	0	2
	Total	237	63	300

Fonte: Elaboração própria.

A implementação de tecnologias de vigilância na região não é algo recente. Apesar do setor de segurança pública e saúde representarem a maior parte dos casos mapeados — em parte devido à digitalização e entusiasmo do setor público em aderir a soluções tecnológicas que possam reduzir o custo humano e financeiro da máquina pública — esses nem sempre foram os principais setores no radar do vigilantismo digital. O levantamento mostra que a implementação de tecnologias de vigilância no âmbito da segurança pública, economia e no setor de transportes já tinham sido reportadas entre os anos de 2010 e 2013 (Gráfico 2). Inclusive, em um estudo que realizamos em 2018 especificamente sobre a implementação de reconhecimento facial no Brasil, já havíamos identificado que projetos-piloto desde o início de 2011 concentravam-se no setor de transportes. Somente a partir de 2018 é que a segurança pública começa a ganhar destaque.[15]

15 Instituto Igarapé (2020). Reconhecimento Facial no Brasil. Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/

Gráfico 2 - Evolução do uso de tecnologias de vigilância (Brasil e América Latina)



Fonte: Elaboração própria[16]

No caso do Brasil, a implementação de tecnologias de vigilância apresenta uma tendência crescente desde 2006, enquanto nos demais países da América Latina os casos reportados permanecem relativamente estáveis até 2016. No gráfico 2, observa-se quatro picos: um em 2010, outro em 2013, 2018 e um logo em 2020. No ano de 2010, diferentes países latino-americanos implantaram tecnologias de vigilância nas atividades policiais. A Colômbia, por exemplo, adotou os dispositivos móveis inteligentes, como os chamados PDA's (*Personal Digital Assistant*) e sistemas como o HEADE (*Spatial Crime Analysis Tool*), para auxiliar nas atividades policiais, desenvolvendo competências analíticas e criminológicas que utilizam georreferenciamento dos principais crimes.

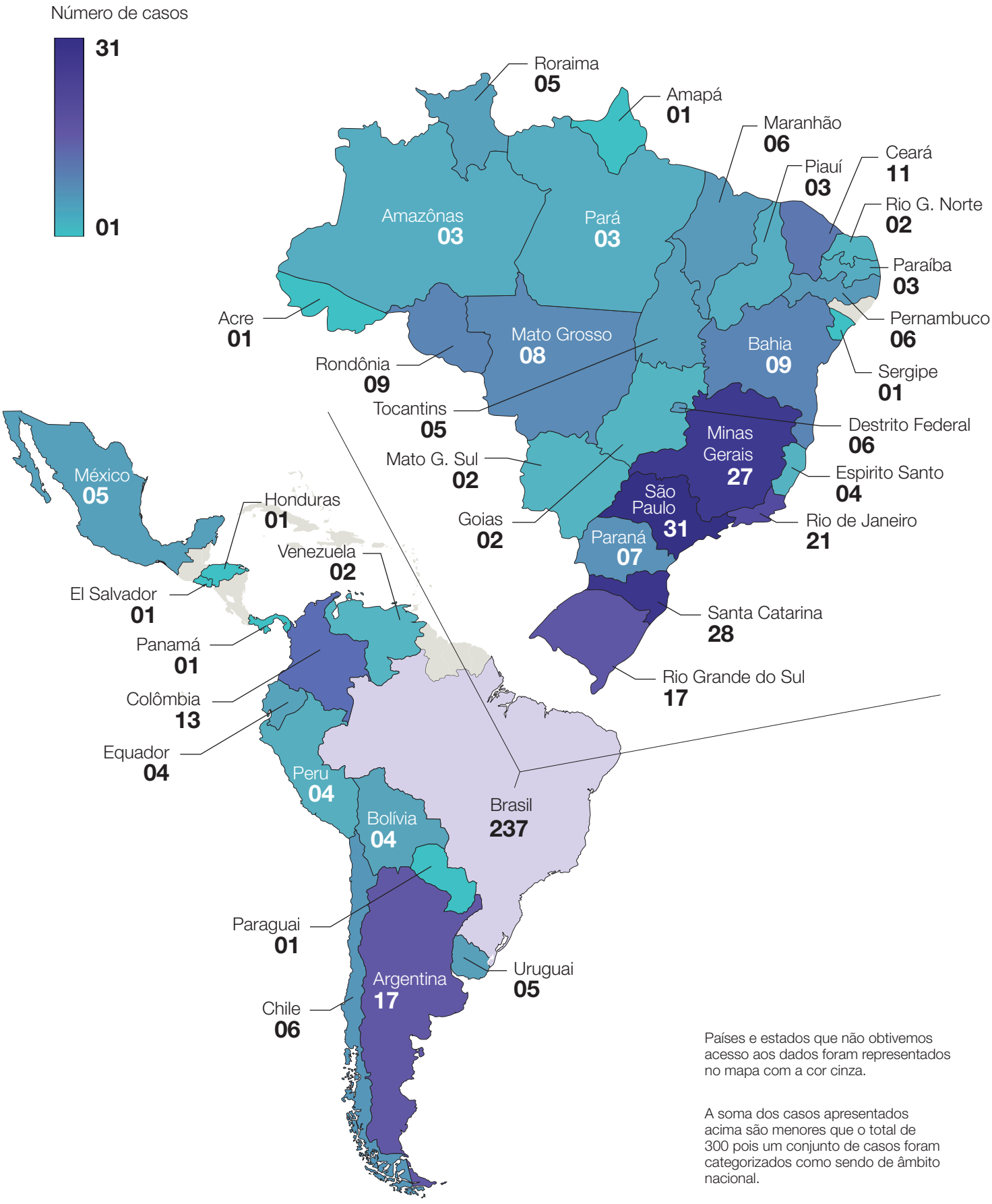
Os anos de 2012 a 2014 foram anos de experimentação, com diversos projetos tecnológicos para monitoramento de fluxos de pessoas, escuta e georreferenciamento, sendo aplicados no contexto dos grandes eventos. No ano de 2018, tecnologias como o reconhecimento facial começam a se espalhar por mais estados do Brasil e para outros setores, como o de transporte.[17]

Já o pico em 2020 deu-se principalmente em razão da crescente implementação e cobertura midiática de projetos de vigilância coletiva desde o início da pandemia. Neste ano, sistemas de reconhecimento facial ganharam robustez em países como Panamá, Uruguai e Argentina. O governo da cidade de Buenos Aires, por exemplo, anunciou a implementação de software de reconhecimento facial na já instalada infraestrutura de videomonitoramento da cidade, indicando que essa funcionalidade ganhou força em toda a região.

16 Observa-se uma frequência menor de casos mapeados na América Latina não devido à sua ausência, mas sim, em função das fontes de dados disponíveis e utilizadas para a coleta de informações serem mais restritas do que as do Brasil. Vale também notar que a contagem de casos para cada setor não é exaustiva e que deve-se considerar que os picos de implementação podem representar tanto um aumento na implementação, quanto um aumento na frequência de reportagem desses casos. Ver nota metodológica Anexo 2.

17 Instituto Igarapé (2020). Reconhecimento Facial no Brasil. Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/

Mapa 1 - Uso de Tecnologias de Vigilância por Países (América Latina) e Estados (Brasil)



Países e estados que não obtivemos acesso aos dados foram representados no mapa com a cor cinza.

A soma dos casos apresentados acima são menores que o total de 300 pois um conjunto de casos foram categorizados como sendo de âmbito nacional.

Gráfico 3 - Uso de Tecnologias de Vigilância por Setor nos Países (América Latina)

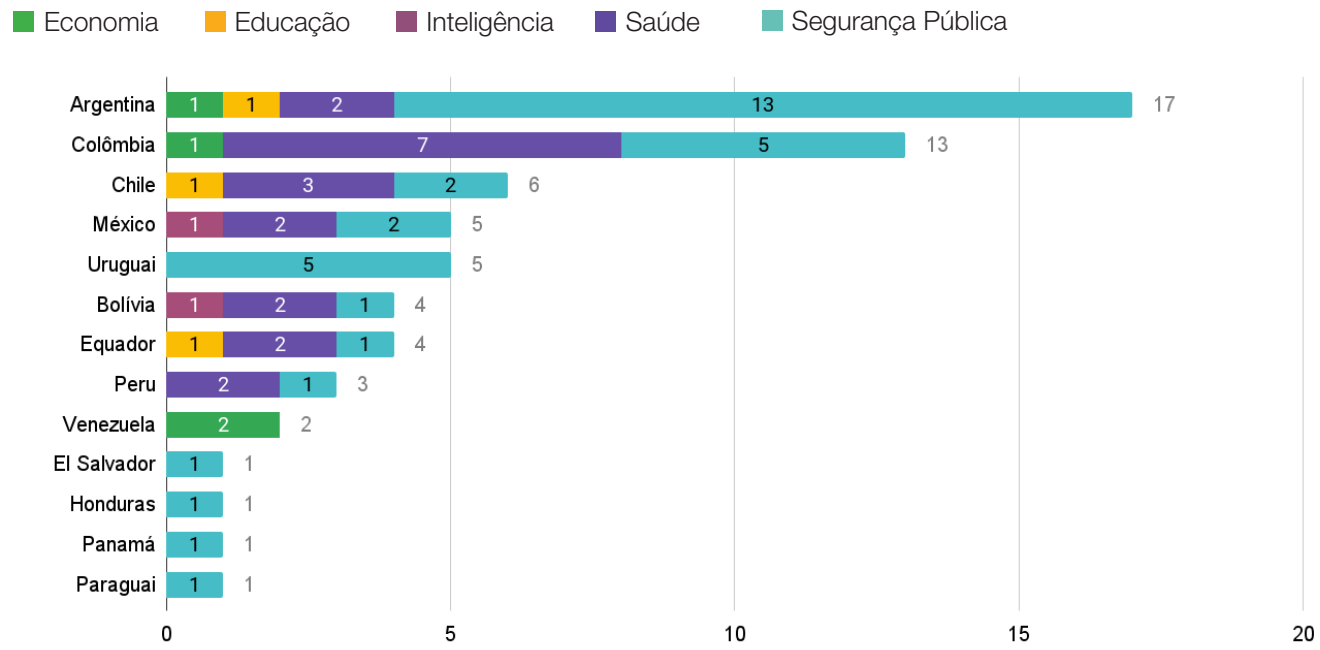
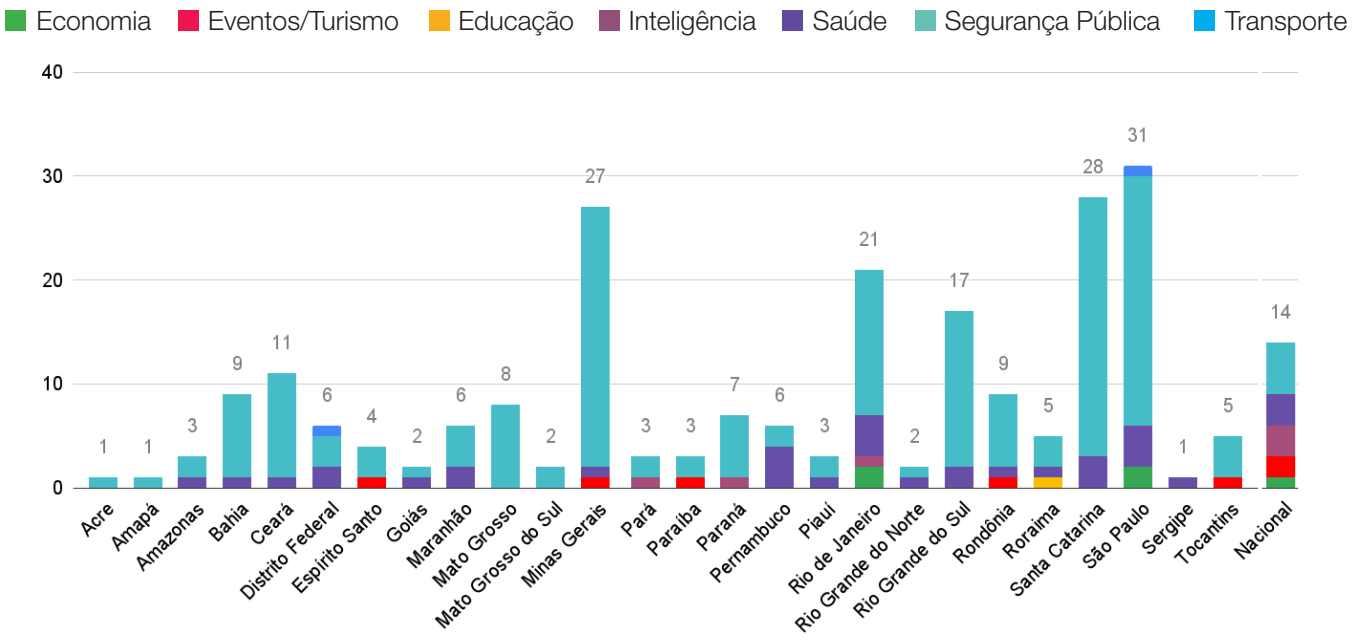


Gráfico 4 - Uso de Tecnologias de Vigilância por Setor nos Estados (Brasil)[18]



Fonte: Elaboração própria

Assim como na América Latina, o ano de 2020 também é emblemático para o Brasil. Os casos reportados naquele ano representam 33,33% do total mapeado. Já no Brasil, observamos uma concentração de implementação de tecnologias dessa natureza no Sul e Sudeste, sendo São Paulo, Santa Catarina, Minas Gerais e Rio de Janeiro – os estados com maior número de casos empregados pelo setor público.

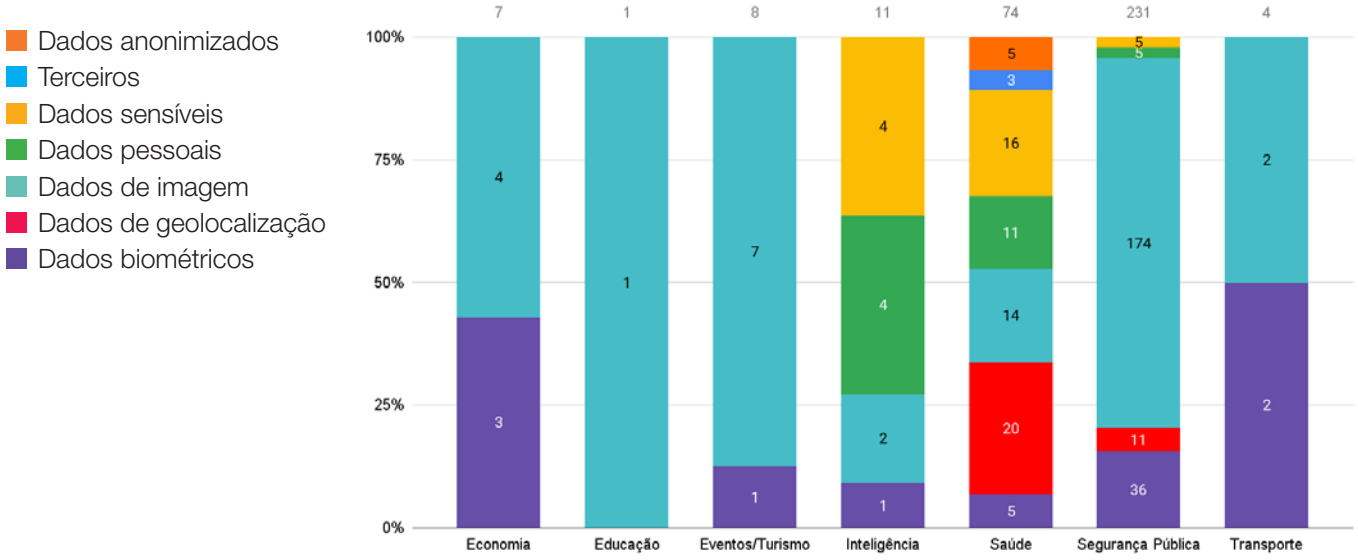
18 No gráfico 4, referem-se a casos nacionais aqueles cujo alcance da tecnologia atinge os 27 estados da federação.

COLETA DE DADOS

O crescente vigilantismo na América Latina e no Brasil reflete, em parte, a proximidade do Estado com empresas de tecnologia. A vigilância, apesar de concentrada na segurança pública, transcende o setor e transborda para outras áreas. Em geral, a vigilância depende da coleta massiva de dados, sejam eles cadastrais, sensíveis, biométricos e/ou geolocalizacionais.

O gráfico 5 apresenta uma visão setorial dos principais tipos de dados coletados nos projetos de vigilância implementados no Brasil. Enquanto nos setores de transporte, segurança pública, educação e eventos/turismo predomina a coleta de imagens decorrentes do vasto uso de videomonitoramento, os setores de saúde e inteligência diversificam o tipo de dados coletados.

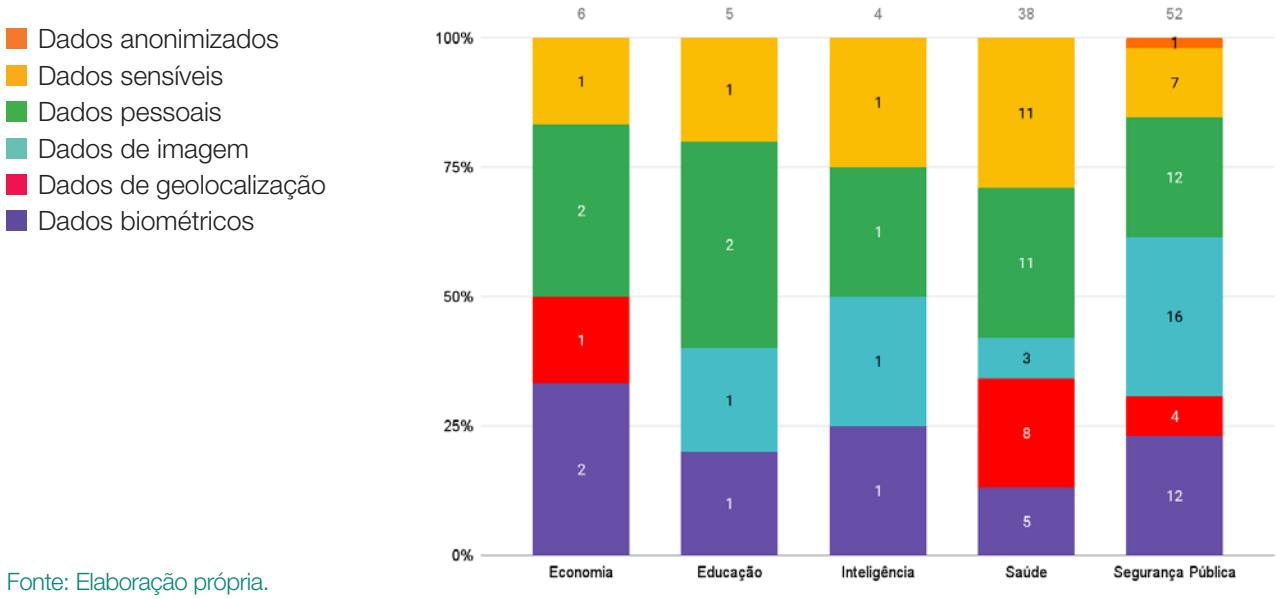
Gráfico 5 - Coleta de dados por setor (Brasil)



Fonte: Elaboração própria.

Na América Latina o cenário é diferente. Em geral, há maior diversidade no tipo de dado coletado em todos os setores, em especial na saúde e na segurança pública. A coleta de dados biométricos avança conforme se aumenta a utilização de tecnologias de reconhecimento facial em toda região.

Gráfico 6 - Coleta de dados por setor (América Latina)



Fonte: Elaboração própria.

Uma visão setorial

A vigilância tornou-se uma prática associada ao funcionamento básico de nossa sociedade cada vez mais digitalizada. Por um lado, estamos mais conectados, acompanhando as redes sociais que se tornaram parte do nosso dia a dia. Por outro, as cidades se transformam em um campo exploratório para a experimentação de novas tecnologias – justificadas pela falta de recursos humanos em polícias, a necessidade de se controlar fraudes de gratuidades em redes de transportes intermunicipais, dificuldade na integração de bases de dados, entre outras razões. Por mais que tecnologias possam auxiliar o Estado no exercício de suas funções, provendo celeridade e capacidade de armazenamento de informações, a implementação permanece experimental, podendo colocar em risco indivíduos, seus dados e os próprios serviços ao cidadão. Sem contar casos mais preocupantes do uso de tecnologias para escuta, monitoramento e vigilância de comunicações e redes sociais – tecnologias essas que, conforme apontado pelo Relator Especial da ONU para a Liberdade de Expressão, podem ser usadas para interferir no direito à privacidade e liberdade[19]. A seguir, apresentamos um panorama de como tem se dado a vigilância em diferentes setores da sociedade, tanto no Brasil como na América Latina.

SEGURANÇA PÚBLICA

A segurança pública utiliza tecnologias de vigilância com diferentes objetivos. Em sua função preventiva, une-se às estratégias e medidas que buscam reduzir a ocorrência de crimes e seus potenciais efeitos para indivíduos e sociedade[20]. Estratégias de prevenção não dependem unicamente da utilização de uma tecnologia (como sistemas de videomonitoramento ou reconhecimento facial), mas devem estar aliadas ao desenvolvimento de protocolos para sua utilização, avaliações periódicas de impacto de direitos humanos e revisão de processos.

Contudo, grande parte dessas tecnologias acabam por alargar o escopo de atuação e capacidade de ação coercitiva das forças de segurança.[21] Conforme apontado na literatura, o vigilantismo presente em práticas de combate a crimes se respalda, em parte, por uma nova visão de policiamento à distância, de classificação e de gerenciamento de grupos de acordo com suas associações com níveis de risco calculados[22]. É nesse contexto que os países (tanto o Brasil como outros da América Latina) concentram-se em empregar tecnologias para prevenire combater crimes. Em sua maioria, os projetos mapeados são caracterizados por essa visão expansiva, seja por abarcar mais de uma tecnologia ou de destacarem múltiplas finalidades para o uso das mesmas. O monitoramento de fluxo de pessoas e objetos e o videomonitoramento são as funcionalidades de maior destaque (ver Gráfico 7)[23].

19 OHCHR Resolution; 2019/A/HRC/41/35

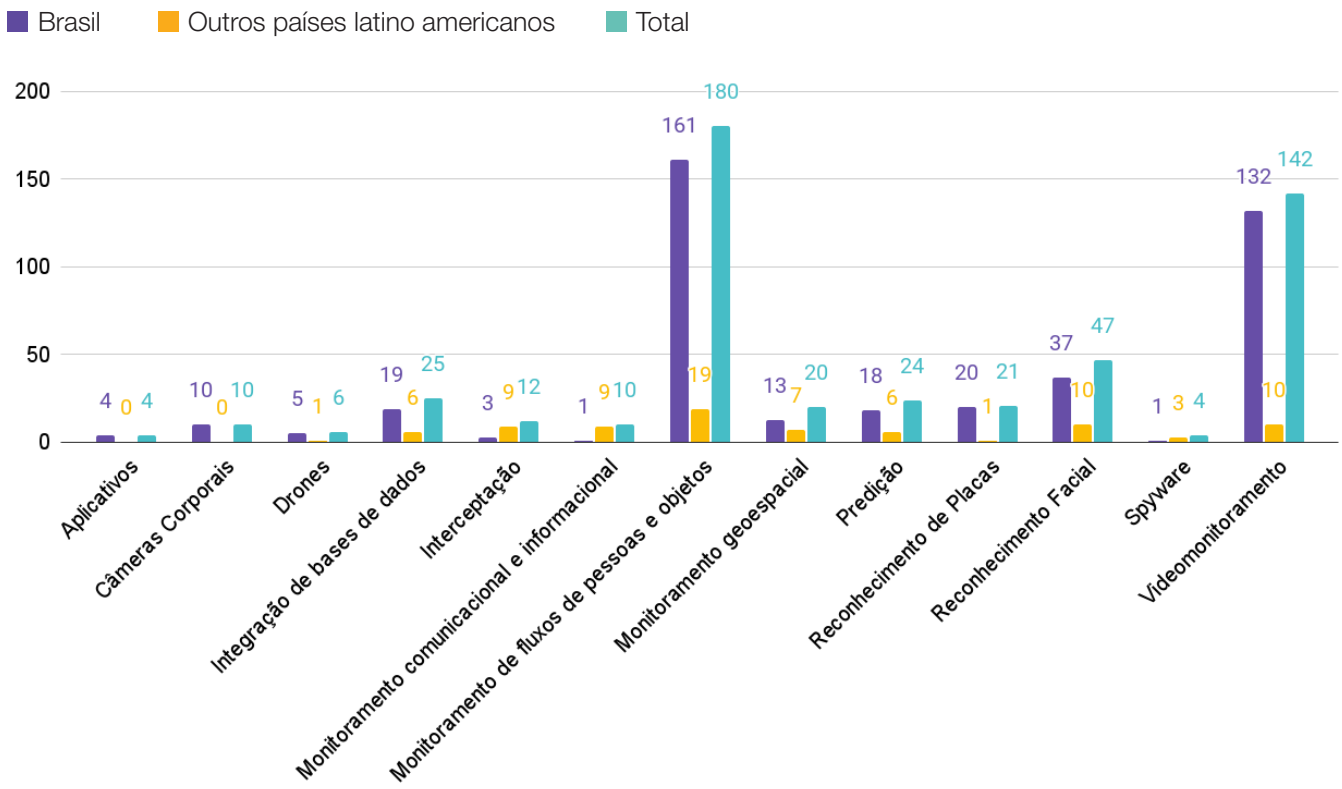
20 ECOSOC Resolution; 2002/13.

21 Byrne, J. & Marx, G., 2011 / Grabosky, P., 1998

22 Haggerty, K.; Wilson, D.; Smith, G.J.D., 2011.

23 Para cada projeto ou caso de implementação de tecnologia de vigilância mapeado, codificamos as diferentes funcionalidades existentes de acordo com o grau de detalhamento e fontes disponíveis sobre o caso. Em geral, identificamos de três a cinco por caso.

Gráfico 7 - Funcionalidades das Tecnologias de Segurança Pública Mapeadas



Fonte: Elaboração própria[24]

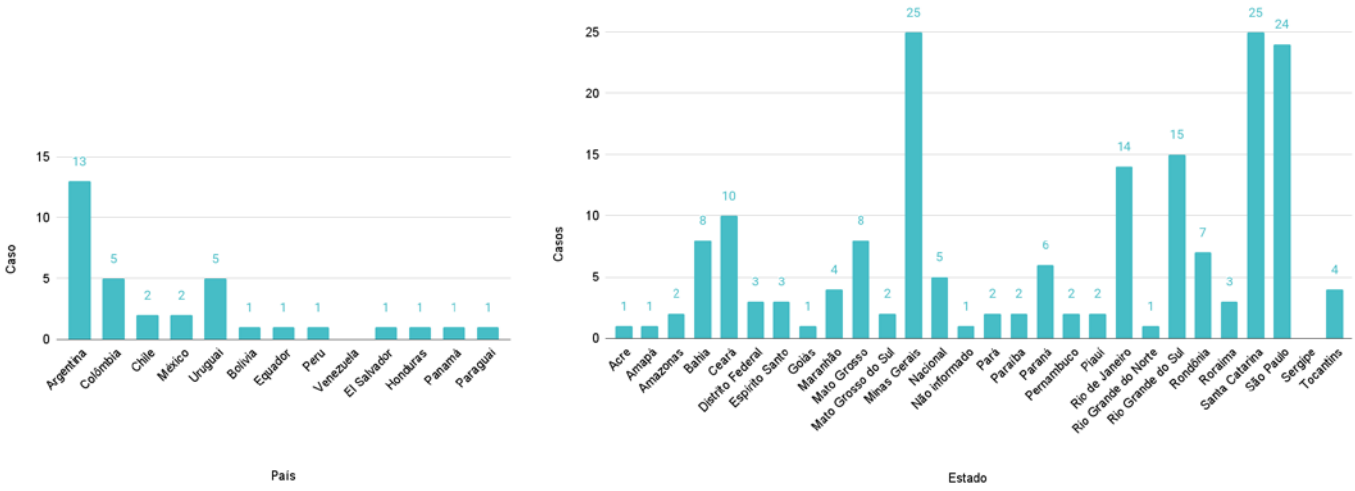
Tanto no Brasil quanto em outros países na América Latina, o setor de segurança pública se destaca como o primeiro colocado na implementação de tecnologias de vigilância, representando 76,4% e 54% dos casos, respectivamente. Tal preponderância não é algo novo. De acordo com nosso mapeamento, no território brasileiro o uso dessas tecnologias pelo setor público cresceu principalmente nos anos de 2010, 2016 e em 2020, ano no qual foi decretada a situação de emergência sanitária em decorrência da pandemia de Covid-19.

No âmbito regional, os casos de uso de tecnologias de vigilância na segurança pública concentraram-se na Argentina, Colômbia e Uruguai (Gráfico 8.1). Já no Brasil, os cinco estados que mais concentram tecnologias do setor são: Santa Catarina, Minas Gerais, São Paulo, Rio Grande do Sul e Rio de Janeiro (ver Gráfico 8.2)[25].

24 Casos de aplicativos, drones e câmeras corporais não foram contemplados no âmbito da América Latina devido à abordagem metodológica desenhada para o mapeamento regional (ver gráfico 7).

25 Constatou-se maior acesso aos dados desses estados, sendo as principais fontes, respectivamente, o Portal da Transparência do Poder Executivo de Santa Catarina, a página de licitações da Polícia Militar do Estado de Minas Gerais, o Tribunal de Contas do Estado de São Paulo (TCE - SP), a página do estado do Rio Grande do Sul no Portal de Transparência nacional e o site de Compras Públicas do estado do Rio de Janeiro.

Gráfico 8 - Casos em Segurança Pública por País (América Latina 8.1 / Brasil 8.2)



Fonte: Elaboração própria

Tendências de implementação e casos de Destaque

Conforme mencionado, tanto o monitoramento de fluxo de pessoas e objetos – 38% dos casos no Brasil e 23% no restante da América Latina – quanto videomonitoramento - 31,1% dos casos totais no setor[26], são as principais funcionalidades dos projetos na região. Importante destacar que o reconhecimento facial e o reconhecimento de placas são funcionalidades que dependem do videomonitoramento. O Projeto Sentinela na cidade de Erechim (RS), destaca-se dentre os casos mapeados de videomonitoramento: ele é um centro de monitoramento construído na Brigada Militar, onde os militares se revezam durante 24 horas para controle das imagens e análise junto à Polícia Civil. Semelhante a outros projetos no Brasil, como o Centro de Operações da Cidade do Rio de Janeiro (COR), o Projeto Sentinela institui um modelo de vigilância apoiado por 216 câmeras espalhadas pela cidade e visa servir como uma ferramenta para a segurança pública[27]. Apesar de idealizado em 2016, o projeto contou com investimentos em 2019 e expansão de sua infraestrutura em 2021. Pouco é reportado publicamente sobre a efetividade e manutenção desses sistemas.

Apesar da tecnologia de reconhecimento facial não ser a principal tecnologia implementada na segurança pública (12,3% dos casos na América Latina e 8,7% no Brasil), analisá-la é essencial, dada a grande controvérsia ao redor desse tipo de tecnologia no mundo[28]. A aplicação do Sistema de Reconhecimento Facial no estado da Bahia tornou-se um dos casos emblemáticos da célere institucionalização da tecnologia nas atividades de segurança pública. Ele começou a ser implementado na capital do estado, no Carnaval de 2019, e teve uma rápida expansão, alcançando 77 municípios em 2021. O investimento foi de cerca de R$ 665 milhões para a instalação de 4.095 novas

26 Dos 161 casos identificados como monitoramento de fluxo de objetos e pessoas no setor de segurança pública, 81,37% refere-se a aplicação conjunta da tecnologia de videomonitoramento, 21,12% a reconhecimento facial, 11,18% refere-se a reconhecimento de placas.

27 Prefeitura de Erechim (2021). Projeto Sentinela Reforça Segurança dos Erechinenses. Disponível em: https://www.pmerechim.rs.gov.br/noticia/15398/13-07-2021/projeto-sentinela-reforca-seguranca-dos-erechinenses

28 Por exemplo: em maio de 2019, São Francisco foi a primeira cidade dos Estados Unidos a banir o uso de tecnologias de reconhecimento facial por agentes de segurança. A decisão tomada por São Francisco virou referência, levando outras regiões a adotarem a mesma proposta como Sommerville, no estado de Massachusetts e Oakland, também na Califórnia. Vide: Carta Capital (2022). De Oakland ao Jacarezinho: os sistemas de reconhecimento facial precisam ser banidos. Disponível em: https://www.cartacapital.com.br/blogs/de-oakland-ao-jacarezinho-os-sistemas-de-reconhecimento-facial-precisam-ser-banidos/#:~:text=A%20legisla%C3%A7%C3%A3o%20federal%20nos%20Estados,em%20seguida%2C%20Oakland%2C%20tamb%C3%A9m%20na

câmeras capazes de identificar criminosos, suspeitos, armas e placas de veículos[29].

Esses e outros casos dependem, cada vez mais, da coleta dos mais diversos tipos de dados. **No Brasil, 68,2% dos casos mapeados coletam dados de imagem[30], seguidos de dados biométricos (14,1%) e dados sensíveis e pessoais em (6,7%).** Nos demais países da América Latina, dados de imagem também foram o tipo predominante dessas tecnologias, figurando em 30,8% dos casos totais.

Um caso relevante mapeado pela pesquisa foi o "Detecta", sistema de monitoramento inteligente desenvolvido pela Microsoft e implementado pelo governo do estado de São Paulo. O Detecta realiza seu monitoramento através do uso de câmeras, alimentando o maior banco de dados de informações policiais da América Latina, conectado-se às bases das polícias civil e militar, do Registro Digital de Ocorrências (RDO), Instituto de Identificação (IIRGD), Sistema Operacional da Polícia Militar (SIOPM-190) e Sistema de Fotos Criminais (FotoCrim), além de dados de veículos e da Carteira Nacional de Habilitação (CNH) do Detran.

Nessa mesma linha de projetos de monitoramento inteligente, a Argentina possui o Programa Integral de Proteção ao Cidadão. Criado em 2009, o Programa integra o plano de segurança pública por meio de contribuições logísticas e da implementação tecnológica em coordenação com os municípios da Província de Buenos Aires. O projeto prevê a implementação de câmeras de videomonitoramento localizadas em vias públicas, assim como sistemas de alarme.

O Detecta realiza seu monitoramento através do uso de câmeras, alimentando o maior banco de dados de informações policiais da América Latina(...)

As imagens captadas pelas câmeras são mantidas pelo município em servidores, por um determinado período de tempo, e podem ser utilizadas a pedido da justiça, como meio de prova para determinados processos.

De acordo com os casos mapeados, as tecnologias de vigilância empregadas na segurança pública na região da América Latina cresceram em 2020, mesmo ano de início da pandemia da COVID-19. A vigilância nos países da região se dá tanto por como de reconhecimento facial, sendo dados de imagem e biométricos os mais requisitados pelo setor. Já a principal funcionalidade da tecnologia empregada é o monitoramento do fluxo de pessoas e objetos, que no Brasil ocorre principalmente pelo emprego de tecnologias de videomonitoramento.

29 Governo da Bahia (2021). Salvador e mais 77 municípios contarão com ampliação de serviço de reconhecimento facial e de placas. Disponível em: http://www.bahia.ba.gov.br/2021/07/noticias/salvador-e-mais-77-municipios-contarao-com-ampliacao-de-servico-de-reconhecimento-facial-e-de-placas/?amp e The Intercept (2021). Lentes Racistas: "Rui Castro está transformando a Bahia em um laboratório de vigilância com reconhecimento facial". Disponível em: https://theintercept.com/2021/09/20/rui-costa-esta-transformando-a-bahia-em-um-laboratorio-de-vigilancia-com-reconhecimento-facial/

30 Cada projeto ou caso mapeado não se restringe à coleta de apenas um tipo de dado (biométricos, sensíveis, imagem, geolocalização, pessoais, terceiros e anonimizados). Para cada caso foram identificados de um a três diferentes tipos de dados coletados, a depender do grau de detalhamento e fontes disponíveis. Na segurança pública no Brasil, foram feitas 255 classificações de tipos de dados, dos quais 68.2% são imagem, 14.1% dados biométricos e 6.7% dados sensíveis e pessoais.

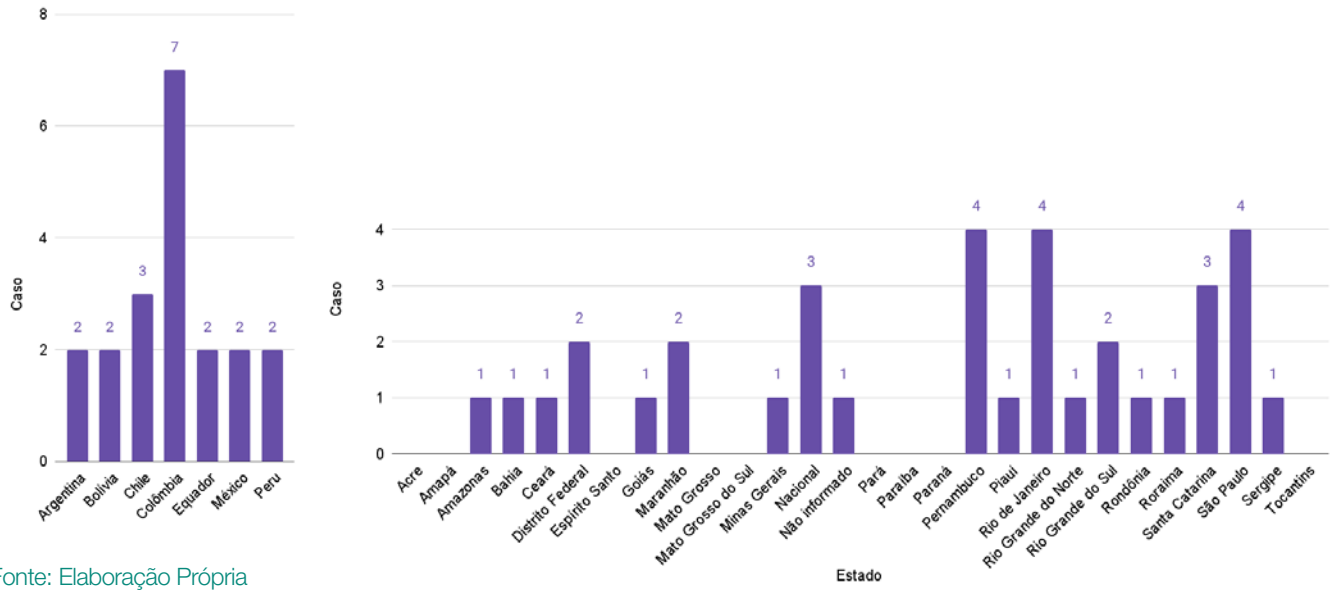
SAÚDE

Desde o início de 2020, diversas tecnologias foram criadas ou adaptadas para combater a pandemia da COVID-19 a nível municipal, estadual, regional e nacional. Nesse contexto, destacam-se dentro do conjunto de casos mapeados projetos direcionados ao (i) desenvolvimento e implementação de diversos aplicativos de autoavaliação, classificação de sintomas e recomendações médicas; (ii) rastreamento de contato com pessoas infectadas pelo Coronavírus; e (iii) utilização de câmeras de vigilância e sistemas de reconhecimento facial para a verificação do uso de máscara e medição de temperatura (câmeras termográficas).

Nesse sentido, configura-se um panorama complexo de expansão da vigilância no contexto da pandemia ancorado na coleta,análise e interpretação sistemática e contínua de dados relacionados à saúde, importantes para o planejamento, implementação e avaliação das práticas de saúde pública.[31]

Dos países da América Latina contemplados pela pesquisa, os casos de implementação de tecnologias de vigilância no setor de saúde representam 31,7% dos casos na América Latina e 14,8% dos casos identificados (ver gráfico 1). Antes da pandemia, vigiar e monitorar pessoas no âmbito da saúde não era uma prática tão aparente no contexto do setor público[32], mas a necessidade de se expandir atividades integradas para monitoramento de sintomas, identificação de áreas de contágio e pessoas infectadas, fez com que se multiplicassem os casos de tecnologias de vigilância entre os anos de 2020 e 2021 na região.

Gráfico 9 - Casos em Saúde (América Latina 9.1 / Brasil 9.2)



Fonte: Elaboração Própria

31 Tradução livre: "*Public health surveillance is 'the ongoing, systematic collection, analysis, and interpretation of health-related data essential to planning, implementation, and evaluation of public health practice' — Field Epidemiology".* Centers for Disease Control and Prevention. Disponível em https://www.cdc.gov/training/publichealth101/surveillance.html.

32 Isso não quer dizer que essas práticas não eram existentes. Historicamente, a digitalização de serviços também levou a um crescimento de novos modelos de negócio no setor privado que buscaram conciliar tecnologia, saúde e bem-estar. Empresas como Amazon e outras "big techs" fornecem acesso facilitado a dispositivos, aplicativos e serviços (Lupton, 2014). Tais estratégias reforçam uma economia da saúde individualizada e baseada em dados que são direcionados para diferentes entidades do setor privado – sejam empresas de tecnologia ou empresas especializadas em saúde (Clarke et al. 2010).

No âmbito regional (gráfico 9.1), a Colômbia destaca-se como maior implementadora de tecnologias de vigilância na saúde, correspondendo a 35% dos casos (ver gráfico 3)[33]. O país implementou projetos que foram desde aplicativos que classificam os usuários de acordo com a gravidade do seu quadro de saúde[34], até drones para o controle da quarentena[35].

Já no Brasil, os estados em destaques na aplicação de tecnologias de vigilância na saúde foram Pernambuco, Rio de Janeiro e São Paulo (ver gráfico 9.2). Tanto no Rio de Janeiro, como em Pernambuco (na cidade de Recife), drones foram utilizados para reforçar o incentivo à quarentena através de um auto-falante que enviava mensagens à população[36]. Junto com São Paulo, essas localidades realizaram o monitoramento de fluxo de objetos e pessoas por meio da coleta sistemática de dados de geolocalização. Por meio do sinal emitido pela antena de celulares, foi possível definir taxas de isolamento social por localidade[37].

Dentre as múltiplas funcionalidades das tecnologias empregadas para prever tanto a efetividade de medidas de controle de emergências sanitárias, quanto auxílio à população na provisão de serviços de saúde, as três principais foram o monitoramento de fluxo de pessoas e objetos, o monitoramento geoespacial e os aplicativos[38] (Ver gráfico 10).

33 Dos 20 casos mapeados de saúde na região latino americana, 7 se encontram no país.

34 O chamado CaliValleCorona é um aplicativo em que os usuários respondem a um questionário que classifica o seu estado de saúde com uma cor (verde, amarelo ou vermelho), de acordo com a gravidade de seus sintomas (Gobernación Valle Del Cauca (2020). Los vallecaucanos cuentan con 'CaliValleCorona', la App que les permitirá realizar una autoevaluación sobre Covid-19. Disponível em: https://www.valledelcauca.gov.co/publicaciones/65721/los-vallecaucanos-cuentan-con-calivallecorona-la-app-que--les-permitira-realizar-una-autoevaluacion-sobre-covid-19/ Arroyo, Verónica in Access Now (2020). Tecnologías de vigilancia para controlar el COVID-19 en América Latina. Disponível em https://www.accessnow.org/tecnologias-de-vigilancia-para-controlar-el-covid-19-en-america-latina/)

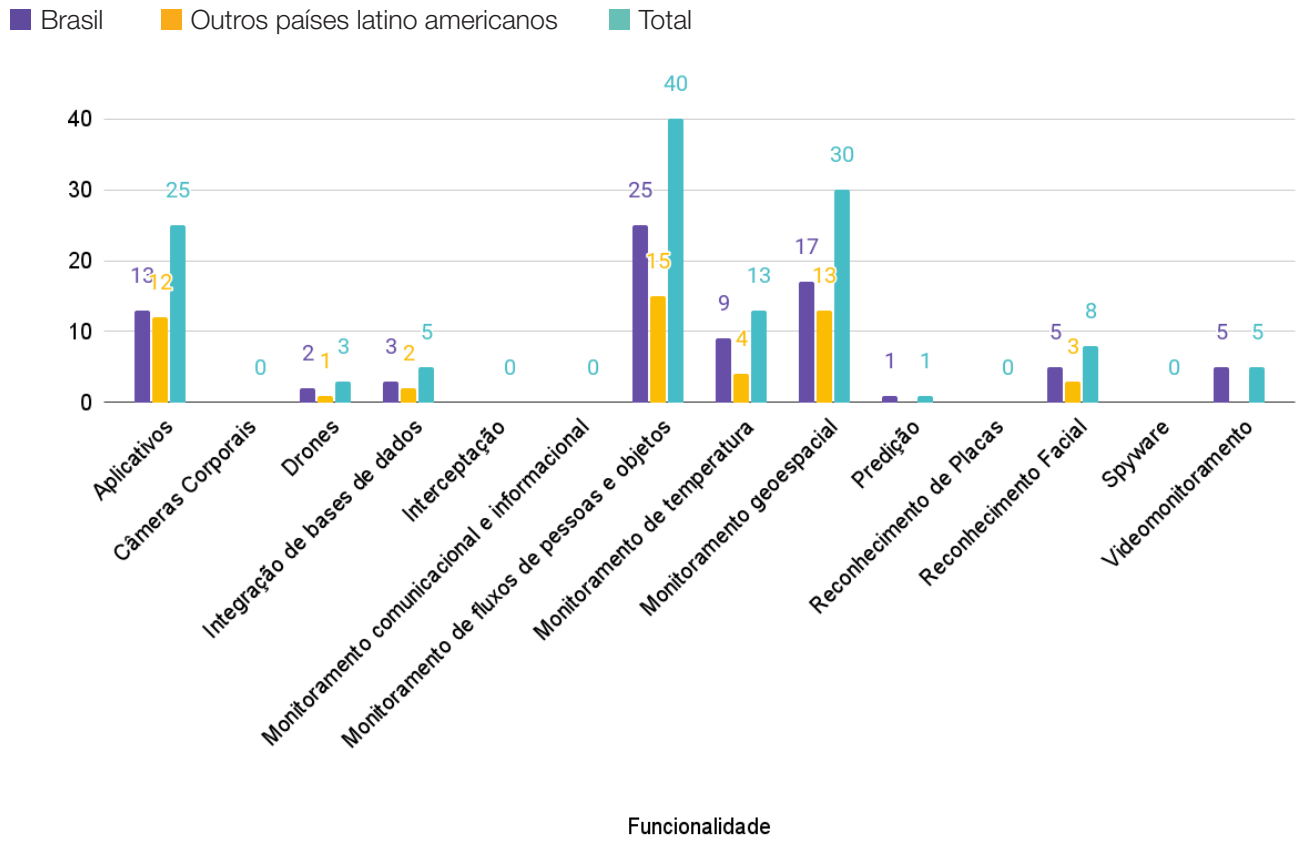
35 A empresa paraguaia Datasystems doou um drone ao Ministério do Interior colombiano, que detectou as funcionalidades de monitoramento de fluxo de pessoas e medição de temperatura. O Drone é equipado com uma câmera que detecta movimento, além de lanterna e alto-falante. (Arroyo, Verónica in Access Now (2020). Tecnologías de vigilancia para controlar el COVID-19 en América Latina. Disponível em https://www.accessnow.org/tecnologias-de-vigilancia-para-controlar-el-covid-19-en-america-latina/ / Extra (2020). Em Bogotá, polícia colombiana usa drones para detectar temperatura e aglomeração. Disponível em https://extra.globo.com/noticias/mundo/em-bogota-policia-colombiana-usa-drones-para-detectar-temperatura-aglomeracao-rv1-1-24437102.html)

36 Prefeitura de Recife (2020). Prefeitura do Recife usa tecnologia como aliada na contenção do novo coronavírus. Disponível em: http://www2.recife.pe.gov.br/noticias/24/03/2020/prefeitura-do-recife-usa-tecnologia-como-aliada-na-contencao-do-novo-coronavirus / Olhar Digital (2020). Covid 19: Prefeitura do Rio usa drone 'falante' contra aglomeração. Disponível em: https://olhardigital.com.br/2020/04/15/coronavirus/covid-19-prefeitura-do-rio-usa-drone-falante-contra-aglomeracoes/

37 A fonte de dados, nesse caso, é o GPS de aparelhos móveis.

38 De acordo com a Tipologia estabelecida pelo Instituto Igarapé, a definição de Aplicativo seria: "Um software ou um programa projetado para desempenhar uma série de funções coordenadas para o fornecimento de um serviço a usuários. Para fins da tipologia, o termo 'aplicativo' se refere a um grupo específico de aplicações desenvolvidas para dispositivos móveis. Nesse sentido, o aplicativo se refere aos múltiplos programas e serviços que são disponibilizados, por exemplo, em repositórios como a Apple ou Google Play Store.". Vide: Instituto Igarapé (2022). Uma tipologia para analisar a implementação de tecnologias de vigilância pelo Estado. Disponível em: LINK

Gráfico 10 - Funcionalidades no Setor de Saúde (Brasil e América Latina)



Fonte: Elaboração Própria

Além disso, tecnologias tipicamente utilizadas para fins de vigilância na segurança pública foram adaptadas para o contexto da pandemia, sendo incorporadas ao setor da saúde. Um exemplo desse processo foi encontrado no metrô da Sé, em São Paulo: através do sistema de reconhecimento facial da empresa Setec, foi possível checar o uso da máscara e auferir a temperatura de até 30 pessoas ao mesmo tempo (caso fosse detectada temperatura acima do 37,5ºC, um sistema de alarme era emitido para funcionários do metrô).[39] Solução semelhante foi instalada em Buenos Aires, onde câmeras de reconhecimento facial controlavam o acesso ao transporte público, mediante a medição da temperatura corporal, o controle da cobertura facial por máscara e a validação das reservas de passagens por meio de um código QR[40]. Na Argentina, no início de 2020, apenas trabalhadores de serviços essenciais podiam usar os transportes públicos e a nova solução de controle de acesso estava conectada diretamente às bases de dados dos trens.

A pesquisa, entretanto, indicou que no contexto de combate à pandemia os aplicativos foram tecnologias indispensáveis. Por exemplo: **Das 50 funcionalidades mapeadas para área da saúde na América Latina, 24% representam os aplicativos, sendo que essa porcentagem é de 16,25% para o Brasil (a partir de um universo de 80 funcionalidades mapeadas no setor no país - ver gráfico 10).** Em termos de

39 G1 (2020). Governo de SP instala câmera que mede temperatura e detecta uso de máscara na estação Sé do Metrô. Disponível em: https://g1.globo.com/sp/sao-paulo/noticia/2020/07/02/governo-de-sp-instala-camera-que-mede-temperatura-e-detecta-uso-de-mascara-em-estacao-de-se-do-metro.ghtml

40 Lobo, Renato in Viatrolebus (2021). Equipamento mede temperatura e uso de máscara em estações de trens argentinas. Disponível em: https://viatrolebus.com.br/2021/02/equipamento-mede-temperatura-e-uso-de-mascara-em-estacoes-de-trens-argentinas/

funcionamento, 84,6% desses aplicativos empregados no campo da saúde no Brasil, tinham como funcionalidade o monitoramento geoespacial e monitoramento de fluxo de pessoas e objetos[41]; na América Latina, essas respectivas funcionalidades estavam presentes em 91,6% e 75% dos casos mapeados[42].

Tendências de implementação e casos de destaque

No Brasil, um exemplo de aplicativo voltado ao monitoramento de geolocalização é o "Monitora Covid", que visa controlar o avanço da pandemia no país. O aplicativo classifica automaticamente o risco de exposição dos respondentes a partir de um questionário[43]. É importante frisar que, nesse caso, o próprio indivíduo se torna a principal fonte de dados ao fornecer deliberadamente dados pessoais e dados sensíveis sobre seu estado de saúde para acessar um determinado serviço, colaborar com iniciativas de saúde, ou saber se está com risco ou não de estar contaminado. No aplicativo, o respondente informava se estava realizando ou não o isolamento social. Dessa forma, por meio do cruzamento de dados da localização informada, conseguia-se saber áreas de maior contágio No processo, todos esses dados tornavam-se anonimizados[44].

Já o aplicativo "Tô de Olho", implementado pela prefeitura de Parnamirim e pelo Governo do Estado do Rio Grande do Norte (RN), disponibilizava uma lista de cidadãos com mais chances de estarem infectados. Após uma análise técnica, a Prefeitura notificava os selecionados e chamava-os para realização da testagem gratuita. Através do aplicativo, os cidadãos também informavam a presença de aglomerações, que era comunicada ao Centro Integrado de Operações de Segurança Pública (CIOSP) da Secretaria de Segurança Pública e Defesa Social do Rio Grande do Norte. Em relação a funcionalidade, o app era capaz de realizar o rastreamento dos contatos, permitindo ter um histórico da localização das pessoas.

Seguindo essa tendência, na Bolívia foi criado um aplicativo semelhante, o chamado "Dr. Sammy Bot", ferramenta que utilizava a localização no Google Maps e a carteira de identidade do usuário para determinar se havia casos de Covid-19 confirmados na área de residência da pessoa. A ferramenta de pré-diagnóstico fazia perguntas sobre os sintomas apresentados e indicava as probabilidades do usuário ter contraído o coronavírus como "significativas" ou "não significativas".

Desde o início de 2020, diversas tecnologias foram criadas ou adaptadas para combater a pandemia da COVID-19, no entanto, dentre as que possuem funcionalidade de monitoramento do fluxo de objetos e pessoas, 28% utilizam monitoramento geoespacial para isso no Brasil[45]. Tendo como fonte de dados o GPS de dispositivos móveis, houve a possibilidade de reconhecimento das áreas mais afetadas pelo Coronavírus, assim como a identificação do contato entre pessoas, o que pôde ser notificado, por exemplo, por mensagens de texto.

41 De um universo de 13 aplicativos em saúde mapeados no Brasil.

42 De um universo de 12 aplicativos em saúde mapeados na América Latina.

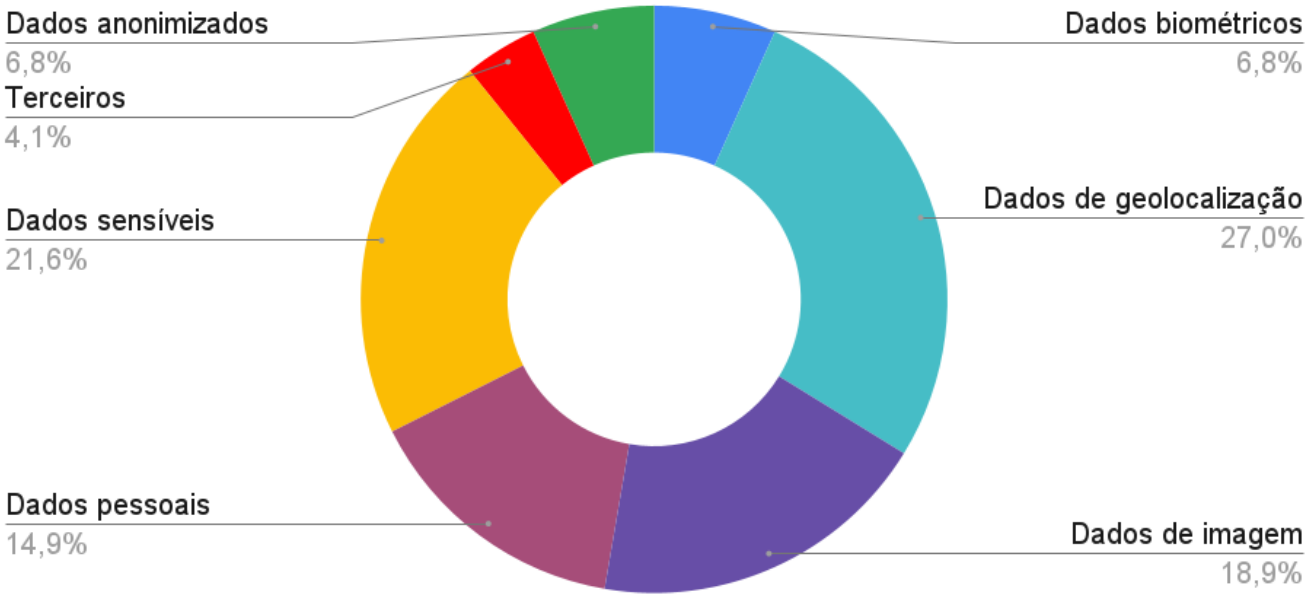
43 Projecto Sonríe #estamosvigilando. Disponível em: https://www.estamosvigilando-cejil.org/pt/inicio/

44 Parecido com esse sistema, o app "Brasil Sem Corona" auxiliou a gestão pública na definição de áreas prioritárias no combate à pandemia, através de experiências com a prefeitura de Caruaru (PE). No app, ao informarem seus sintomas, os cidadãos ajudavam na construção um mapa digital de risco epidemiológico.

45 De um universo de 25 casos de saúde que realizam monitoramento de fluxo de objetos e pessoas mapeados na América Latina.

Devido à variedade de tecnologias aplicadas, há também no setor de saúde uma diversa gama de dados sendo coletados, configurando-se como o setor mapeado que mais coleta diferentes tipos de dados no Brasil[46]:

Gráfico 11 - Tipos de Dados Coletados pelo Setor de Saúde (Brasil)



Fonte: Elaboração Própria

Na América Latina, os dados mais coletados pelo setor de saúde foram: dados sensíveis e pessoais (28,9%), geolocalização (21,1%), e imagem (7,9%)[46]. A pandemia instaurou no setor da saúde a necessidade de se vigiar áreas geográficas de contágio, sendo, em muitos casos, o indivíduo o principal fornecedor desses dados (a exemplo dos questionários de saúde mencionados).

Dessa forma, o monitoramento de fluxo de pessoas tornou-se essencial na saúde. Isso ocorre não somente por aplicativos que realizam rastreamento de contato, mas também por câmeras de videomonitoramento e sistemas de reconhecimento facial que, além da captura de imagens e dados biométricos, captam dados sensíveis, como a temperatura corporal das pessoas.

Do ponto de vista do desenvolvimento das tecnologias, destaca-se a cooperação público-privada, especialmente no monitoramento geoespacial. Os dados de geolocalização foram imprescindíveis no exercício da vigilância em saúde durante a pandemia. Além disso, a saúde é o setor que capta uma maior variedade de dados no Brasil, dentre eles os dados de GPS, informações pessoais e sensíveis.

46 No caso do setor de saúde, na América Latina, os casos levaram a um universo de 38 classificações de tipos de dados mapeados pelo setor.

Cooperação Público-Privada no Combate à Pandemia

Em nosso mapeamento, dos 237 casos mapeados no Brasil, 4,22% referem-se a projetos cujo desenvolvedor forneceu tecnologia via cooperação público-privada. Nesse contexto, tanto organizações públicas, quanto entidades privadas desenvolvem conjuntamente um tipo de tecnologia, assumindo diferentes responsabilidades nesse processo. Durante a pandemia da COVID-19, a cooperação público-privada foi um elemento central no desenvolvimento de iniciativas tecnológicas para a administração da pandemia. Veja a seguir como:

- **MONITORAMENTO GEOESPACIAL NO COMBATE A PANDEMIA**: entre as experiências mapeadas estão a cooperação entre a empresa InLoco e as prefeituras do Rio de Janeiro e de Recife; e o caso das empresas de telefonia Claro, Oi, Tim e Vivo com o Governo do Estado de São Paulo, no qual trabalharam para que o sinal emitido pelas antenas de celulares possibilitasse o monitoramento geoespacial. Nessas iniciativas é possível medir o grau de isolamento social a partir de dados georreferenciados agrupados. No caso do SIMI-SP (Sistema de Monitoramento Inteligente), "uma central de inteligência analisa dados de telefonia móvel para indicar tendências de deslocamento" das pessoas (Governo de São Paulo). Em Recife, os dados coletados geraram um índice de isolamento por bairro, indicando aqueles que mais respeitaram a quarentena e quais tiveram maior fluxo de pessoas[48].

- **APLICATIVOS DE SAÚDE COMO TENDÊNCIA**: considerando a necessidade de isolamento social e restrição da mobilidade exigidos pela pandemia, vários aplicativos foram criados no contexto de cooperação público-privada. Para além de oferecerem o monitoramento geoespacial e de fluxo das pessoas, eles também indicam os serviços de saúde mais próximos e o status sanitário da localização do usuário. Dentre os casos levantados, destacam-se a parceria entre o Governo do Amazonas, o Instituto Transire, a SASI Comunicação Ágil e a Universidade Estadual do Amazonas para desenvolvimento do aplicativo "Juntos no Combate- COVID 19"[49] e a parceria entre a Fundação Estatal Saúde da Família (FESF-SUS), Secretaria de Ciência, Tecnologia e Inovação (SECTI) do Estado da Bahia, a Secretaria de Saúde do Estado da Bahia (SESAB) e as empresas Novetech e Core para a construção do "Monitora Covid", que surgiu na região nordeste e amplificou seu uso.

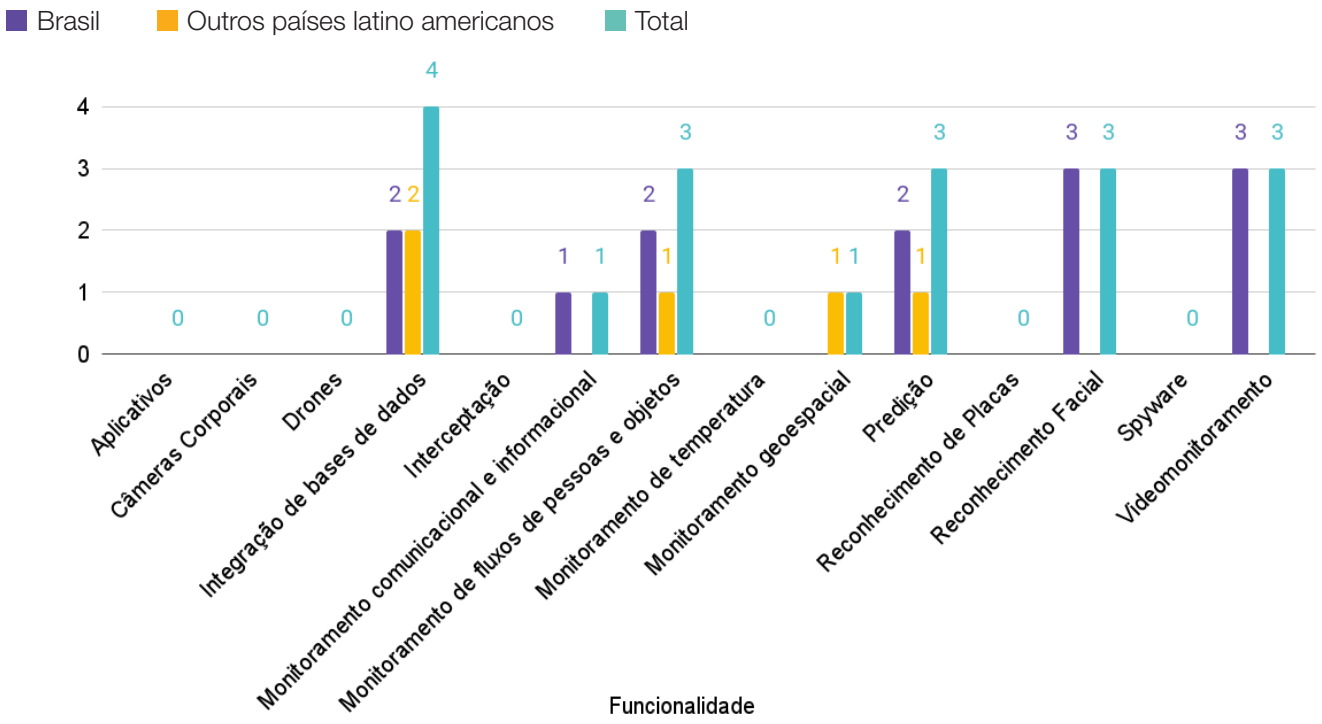
47 Prefeitura de Recife (2020). Prefeitura do Recife usa tecnologia como aliada na contenção do novo coronavírus. Disponível em: http://www2.recife.pe.gov.br/noticias/24/03/2020/prefeitura-do-recife-usa-tecnologia-como-aliada-na-contencao-do-novo-coronavirus

48 Venturini & Souza (2020).

ECONOMIA

Nesse setor foram mapeadas tecnologias associadas ao controle tributário e o acesso a benefícios que inclui, mas não se restringe a, por exemplo, sistemas do governo para auxiliar no controle de informações de beneficiários de programas sociais.

Gráfico 12 - Funcionalidades Tecnológicas no Setor de Economia (Brasil e América Latina)



Fonte: Elaboração Própria

Tendências de implementação e casos de destaque

É relevante notar que no Brasil as principais funcionalidades de tecnologia de vigilância empregadas no setor da economia são as de reconhecimento facial e videomonitoramento. Nos demais países da América Latina, a função de integração de base de dados e predição aparece em destaque. Selecionamos alguns casos nos quais a integração de base de dados é utilizada como meio de vigilância no setor econômico.

No Brasil, a solução tecnológica NeoFaceWatch, que possui funcionalidades de predição, reconhecimento facial, videomonitoramento e monitoramento de fluxo de pessoas e objetos, foi instalada em 14 aeroportos internacionais brasileiros[49]. A tecnologia conta com serviços de integração de sistemas e manutenção existentes para o órgão específico da Receita Federal. Graça à essa integração é possível identificar passageiros que foram registrados por atividade suspeita, atuando assim no controle das fronteiras[50].

49 NEC (2015). NEC to provide facial recognition systems for 14 international airports in Brazil. Disponível em https://www.nec.com/en/press/201507/global_20150716_02.html

50 Digital Security Magazine. Aeroportos internacionais do Brasil implementam tecnologia de reconhecimento facial NEC. Disponível em: https://www.digitalsecuritymagazine.com/pt/2015/07/30/aeropuertos-internacionales-de-brasil-implantan-la-tecnologia-de-reconocimiento-facial-de-nec/

Na Venezuela, em 2018, o governo contratou a empresa ZTE para implantar um programa semelhante ao chamado "*carnet de la patria*"[51]. Os cartões são usados para conceder subsídios alimentares, fornecer acesso a serviços de saúde e administrar outros programas sociais. Na Colômbia, também há o emprego da mesma funcionalidade de integração de base de dados para liberação de benefícios sociais à população: o sistema Renda Solidária já identificou cerca de três milhões de famílias afetadas pela pandemia que receberam um subsídio de, em média, COP 160.000 (aproximadamente R$ 200). É importante frisar que os beneficiários foram identificados a partir do cruzamento de informações contidas no Sistema de Seleção de Beneficiários para Programas Sociais (SISBEN). O estudo de Joan López (2021) revela como o sistema conecta diferentes dados de modo a identificar quais são os perfis de futuros beneficiários. Dependendo da pontuação recebida, as famílias são identificadas como elegíveis para programas sociais implementados por diferentes órgãos. O programa Renda Solidária, contudo, construiu um novo Banco de dados, no qual o Escritório de Desenvolvimento Nacional (NDO) "mesclou" diferentes registros administrativos usando os mais diversos dados gerenciados não só por atores públicos, mas por particulares. É mais um exemplo de tecnologia adaptada ao contexto da pandemia.

INTELIGÊNCIA

No âmbito das atividades de inteligência, observa-se a utilização de tecnologias para as mais variadas finalidades. Os casos mapeados vão desde o emprego de tecnologias para auxiliar na construção de uma base de dados de eleitores "confiáveis" através do uso de bases biométricas (feito pelo Tribunal Nacional Eleitoral da Bolívia em 2009)[52] ao controle migratório em fronteiras. A Agência Brasileira de Inteligência (ABIN), por exemplo, possui informações geradas pelo projeto "FronteiraTech", sistema instalado pela Agência Brasileira de Desenvolvimento Industrial (ABDI) na divisa entre o Brasil e o Paraguai.[53] No entanto, os casos de destaque nesse setor estão associados a espionagem de e por pessoas e governos através de celulares, sinais telefônicos, computadores e ferramentas Open Source Intelligence (OSINT)[54].

O setor de inteligência ao qual nos referimos nesse documento abarca as agências de inteligência e órgãos correlatos envolvidos em atividades de inteligência para fins de segurança nacional e segurança pública. **No Brasil, o emprego desse tipo de tecnologia no setor representa 2,5% dos casos mapeados e, na América Latina, esse número é de 3,2% (ver gráfico 1). O baixo percentual de casos identificados pode estar atrelado à falta de transparência própria desse setor. Contudo, os casos reportados, possuem um alto potencial de uso excepcional além dos riscos a direitos inerentes ao emprego de tecnologias de vigilância no contexto de atividades de inteligência.** Apesar dos poucos casos, destaca-se a variedade de tecnologias empregadas, conforme gráfico 13.

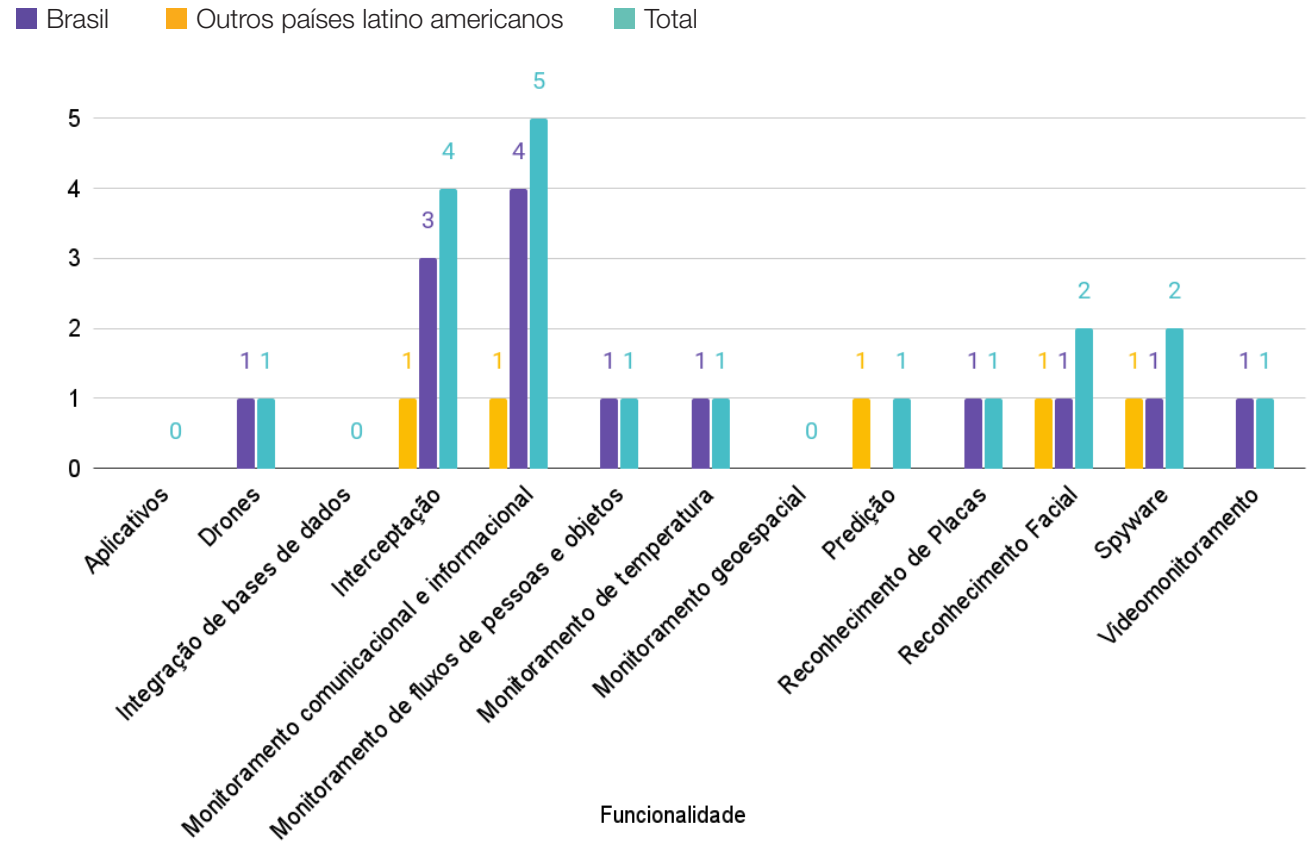
51 Mecanismo de controle biométrico que limita as compras de produtos e alimentos nos supermercados da Venezuela, sistema implementado pelo presidente Nicolás Maduro.

52 Frost & Sullivan, 2016.

53 ABDI, 2021.

54 Coleta de informações e inteligência em fontes abertas.

Gráfico 13 - Funcionalidades Tecnológicas no Setor de Inteligência (Brasil e América Latina)



Fonte: Elaboração Própria

No Brasil, a interceptação e o monitoramento comunicacional se destacam no tipo de funcionalidade mapeada. Já na América Latina, não há preponderância entre elas.

Ao longo dos últimos anos, muitos governos têm buscado ampliar o rol de ferramentas com o objetivo de monitorar grupos opositores e dissidentes políticos. Diferente da interceptação, que é realizada mediante um mandado judicial ou sob supervisão administrativa, o spyware é caracterizado pela desproporcionalidade de acesso que é conferida ao atacante, mediante a injeção de um malware em um dispositivo. O spyware é um dos exemplos notórios do uso abusivo de tecnologias para a execução de práticas de hacking governamental[55], isso é, perseguição de dissidentes de governos, grupos da sociedade civil, ativistas, jornalistas, organizações acadêmicas, entre outros.

55 Hacking governamental se refere à manipulação oculta e a interferência com dispositivos e softwares de indivíduos por entes governamentais. Além do spyware, outras atividades associadas ao hacking governamental são: uso de código malicioso desenvolvido por entes estatais; estocagem ou exploração de vulnerabilidades por governos e flexibilização da criptografia. Um exemplo é a estocagem ou compra de vulnerabilidades críticas, também chamadas de “zero-days” ou “0-days”. Essas vulnerabilidades, quando exploradas para fins maliciosos, ou seja, quando deixam de ser somente para o conhecimento de uma vulnerabilidade, e passam a ser uma ‘exploit’ do governo, também podem vir a ser chamadas de armas cibernéticas. Por vezes, o acúmulo de vulnerabilidades críticas é justificado por uma competição geopolítica e, portanto, entre Estados. Contudo, quando essas capacidades são utilizadas para grupos dentro de um país ou quando um outro Estado utiliza-se dessa ferramenta para atingir um grupo da sociedade de outro país, o desafio torna-se maior do que simplesmente ‘hacking governamental’ e pode vir a acionar a aplicabilidade do Direito Internacional em casos de atividades inter-estatais (Privacy International, Disponível em: https://privacyinternational.org/learn/government-hacking)

Um exemplo dessa tecnologia que ficou conhecida internacionalmente é o malware Pegasus, desenvolvido pela NSO Group e capaz de invadir smartphones sem que o usuário acesse um link específico. Em 2018, a organização Citizen Lab publicou um estudo[56] no qual foram identificadas suspeitas de infecções do Pegasus em 45 países, sendo um deles o Brasil. Não se sabe quem teria comprado a ferramenta, mas "o mesmo comprador que usou o Pegasus no Brasil também deixou rastro digital em Bangladesh, Hong Kong, Índia e Paquistão. As infecções em território brasileiro foram associadas à Telemar Norte Leste S.A., que pertence à Oi"[57].

A empresa NSO Group esteve no centro do debate brasileiro sobre vigilância, quando foi anunciado, em maio do ano passado, o Pregão Eletrônico 3/2021 do Ministério da Justiça, voltado à aquisição de solução de inteligência em fontes abertas, mídias sociais, e deep e dark web. Após grande repercussão nacional, a empresa deixou a disputa e a tecnologia vencedora do pregão, diferente do spyware Pegasus, foi uma ferramenta de OSINT da Harpia Tech, com alta capacidade de perfilação dos dados captados, podendo representar riscos quanto ao cruzamento de dados de cidadãos e grupos alvos específicos. Em demais países da América Latina foi emblemática a revelação de que o software estava sendo usado pelo governo do México, ainda sob a gestão de Enrique Peña Nieto, para espionar ativistas contrários à sua gestão, sendo uma ferramenta usada desde 2011.

56 Marczak et al, 2018

57 El País (2019). Vírus para espionagem política denunciado pelo WhatsApp foi usado no Brasil. Disponível em: https://brasil.elpais.com/brasil/2019/05/15/tecnologia/1557877977_241967.html .

Expansão da vigilância entre setores: Segurança pública e Inteligência

Spyware e monitoramento comunicacional

O spyware é um termo utilizado para descrever quando um código malicioso (malware) é utilizado para espionar atividades realizadas por dispositivo móvel ou um computador. A utilização do código malicioso permite o acesso privilegiado por parte do atacante às atividades de um indivíduo, podendo coletar e vigiar redes sociais, serviços de mensageria privada, senhas, contas bancárias, sem que este esteja ciente. Essa tecnologia ganhou destaque em julho de 2021 quando diferentes organizações da sociedade civil e consórcios jornalísticos denunciaram a comercialização e uso do spyware Pegasus da NSO Group, empresa israelense[59]. É importante frisar que na pesquisa das funcionalidades identificadas em segurança pública, tanto no Brasil como em demais países da América Latina, também há tecnologias empregadas para atividades de interceptação, monitoramento comunicacional e implementação de spywares. Apesar do número baixo, o uso dessas ferramentas na segurança pública acende um alerta em relação à capacidade de monitoramento de grupos e indivíduos pelo poder público. Sem as salvaguardas e controle necessários, essas atividades podem representar um risco aos cidadãos. No Brasil, por exemplo, foi emblemática a compra pela Polícia Federal do software Remote Control System (RCS)/ Galileo, da empresa Hacking Team, por intermédio da empresa YasniTech, para utilização em um projeto piloto em 2015. Na Colômbia, o Galileo também foi adquirido pela Direção da Polícia Nacional (DIPON), destacando-se o fortalecimento da Plataforma Única de Monitoramento e Análise (PUMA), ligada à Dirección de Investigación Criminal e Interpol de la Policía (DIJIN) e que tem por finalidade registar ou verificar informação de pessoas ligadas a investigações judiciais[60]. No que tange o uso de outras ferramentas de monitoramento comunicacional e informacional, é importante destacar o uso no Brasil, Honduras, El Salvador e na Argentina do dispositivo Universal Forensic Extraction Device (UFED), capaz de extrair dados armazenados e removidos de telefones celulares, computadores e outros dispositivos móveis, para fins de investigação forense.

58 Uma lista com 50 mil números de telefone de cidadãos que teriam sido monitorados pelo software Pegasus vazou na imprensa em julho de 2021 tendo sido revelada por uma investigação conjunta realizada pelas ONG's Forbidden Stories e a Anistia Internacional. As denúncias foram divulgadas nos veículos Washington Post, Guardian, Le Monde e outras 14 outras mídias (BBC, 2021).

59 Acha, 2016

OUTROS SETORES

Transportes

Apesar de menos noticiado, os casos de implementação de tecnologias de vigilância no setor de transportes são uma das mais antigas no contexto brasileiro. Conforme apontamos em nosso levantamento de aplicação de reconhecimento facial, o setor de transportes foi um dos primeiros a experimentarem tecnologias como essas[60].

As aplicações nessa área são variadas: emaeroportos, por exemplo, determinados aplicativos combinam validação biométrica com a análise de dados no check-in, vinculando o nome e a foto dos passageiros ao seu CPF; câmeras com reconhecimento facial permitem identificação de pessoas, contribuindo para a segurança e controle do local; e totens de atendimento realizam a mensuração da temperatura corporal dos passageiros no embarque e desembarque internacional. A tecnologia de reconhecimento facial também permite a validação de gratuidades no ônibus e bloqueio em caso de uso indevido.

Destacamos dois casos no setor de transportes, cujas principais funções concentram-se no monitoramento do fluxo de pessoas e objetos por meio de aplicativo e sistemas de reconhecimento facial. Por exemplo, ônibus de São Paulo captam imagens dos passageiros quando esses passam pelas catracas validadoras de bilhete e bloqueiam o cartão caso a imagem do passageiro não seja a mesma do cadastro. Até 2019 já haviam sido bloqueados 331.651 cartões de Bilhete Único[61]. O aplicativo "Embarque + Seguro", desenvolvido pelo Serviço Federal de Processamento de Dados (Serpro)[62], começou a ser usado no Aeroporto Internacional de Brasília. Por meio dele, as empresas aéreas conseguem fazer o cadastramento do passageiro na hora do check-in, vinculando sua foto a dados pessoais, como CPF, combinando análise biométrica e comparando com dados do Denatran e do Barramento SGD (TSE)[63]. Desde outubro de 2020 a tecnologia já foi testada em outros terminais aéreos, como o de Florianópolis (SC), Salvador (BA), Belo Horizonte (Confins), Rio de Janeiro (Santos Dumont) e São Paulo (Congonhas), pelas companhias Latam, Gol e Azul.

O que esses casos ilustram é a normalização da utilização e coleta de dados biométricos (o registro facial) em transportes que carecem de transparência sobre o tratamento e coleta dos dados dos cidadãos e de relatórios de impacto social sobre essas práticas.

---

60 Instituto Igarapé (2020). Reconhecimento Facial no Brasil. Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/

61 Folha de São Paulo (2019). Reconhecimento facial bloqueia 331 mil Bilhetes Únicos em SP: Tecnologia foi instalada nas catracas para evitar fraudes. Disponível em https://agora.folha.uol.com.br/sao-paulo/2019/06/reconhecimento-facial-bloqueia-331-mil-bilhetes-unicos-em-sp.shtml

62 Crypto ID (2021).Governo Federal testa Embarque + Seguro no Aeroporto de Brasília. Disponível em https://cryptoid.com.br/governo-digital-government/governo-federal-testa-embarque-seguro-no-aeroporto-de-brasilia/

63 Saiba mais em: https://campanhas.serpro.gov.br/embarque-mais-seguro/#:~:text=M%C3%ADdia%20Kit-,O%20que%20%C3%A9%3F,as%20viagens%20a%C3%A9reas%20mais%20seguras.

Expansão da viligância entre setores: Transporte e Segurança pública

A aplicação de algumas tecnologias mapeadas podem estar presentes na interseção de dois ou mais setores. Os sistemas de videomonitoramento e reconhecimento facial no setor de transporte[65] também identificam crimes como fraudes em bilhete único e furtos nas dependências do transporte, além de permitir a identificação de pessoas procuradas pela polícia entre os passageiros. Um exemplo desse tipo de uso compartilhado é a instalação de câmeras de videomonitoramento nas vias 11 (Coral) e 12 (Safira) da Companhia Paulista de Trens Metropolitanos (CPTM)[66], em São Paulo. De acordo com a licitação de TC-046391/026/13, a Companhia Paulista de Trens Metropolitanos - CPTM contratou a empresa Power Segurança e Vigilância Ltda com o objetivo de prestação de serviços de segurança e vigilância nas instalações de trens[67], ou seja, em um contexto de fornecimento de serviço de transporte público, há também a aplicação de tecnologias de vigilância para fins de segurança. Dos 181 casos de segurança pública no Brasil, 10 apresentam intersecção com o setor de transportes.

Educação

Dos casos encontrados sobre aplicação de tecnologias de vigilância na América Latina, 4,8% referem-se ao setor da educação com destaque à utilização das mesmas para as seguintes funções: integração de base de dados e predição (28,6%) e monitoramento de fluxo de pessoas (14,3%).

Em relação à funcionalidade de integração de bases de dados e predição, há a noção de que essas tecnologias ajudam a identificar alunos em maior situação de vulnerabilidade, prevenindo deserção escolar a partir do monitoramento de indicadores de risco, associados com o ingresso ao sistema educacional. Além disso, um dos principais desafios para a utilização de tecnologias preditivas e de vigilância no contexto do setor de educação refere-se à coleta sistemática de dados pessoais de pessoas menores de idade. Abaixo, apresentamos alguns casos identificados no levantamento:

- **ARGENTINA**: Na cidade de Salta, o Ministério de Primera Infância do Governo, usou uma tecnologia da Microsoft para implementar um sistema que permite o monitoramento para prevenção da gravidez em adolescentes e analisa índices de deserção escolar. Os dados processados pela empresa de softwares indicam quem seriam as adolescentes com essa maior probabilidade. “De acordo com a empresa, a partir de dados coletados por meio de enquetes, ‘algoritmos inteligentes’ permitem identificar características nas pessoas, que podem derivar em algum desses problemas e advertir o governo para que possa trabalhar na sua prevenção” (Venturini, 2019)[67].

64 Instituto Igarapé (2020). Reconhecimento Facial no Brasil. Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/

65 Tribunal de Contas do Estado de São Paulo, 2013. Disponível em: http://www2.tce.sp.gov.br/arqs_juri/pdf/497922.pdf

66 Vide: http://www2.tce.sp.gov.br/arqs_juri/pdf/497922.pdf

67 Venturini, 2019.

- **CHILE**: Foi implementado o Alerta Niñez/ Childhood Alert System (Sistema Alerta Niñez – SAN), sistema que se baseia no processamento estatístico de grandes quantidades de dados provenientes de órgãos públicos, para qualificar a população menor de 18 anos, indicando a probabilidade de sofrer violações[68].

O setor de educação nem sempre é o primeiroque se associa à utilização de tecnologias de vigilância. No entanto, os últimos anos foram marcados por projetos piloto de implementação de reconhecimento facial em escolas, visando garantir maior controle de presença. Vale refletir se o uso de tecnologias dessa natureza no ambiente escolar não cria um incentivo perverso, isto é, constrói um ambiente de controle ao invés de incentivos positivos para a permanência na escola. Além disso, o uso de tecnologia de forma isolada não resolverá os problemas de vulnerabilidade identificados. Ela precisa estar conectada com políticas que possam assistir estudantes em situações de risco.

Eventos/Turismo

O setor de eventos/turismo inclui os órgãos públicos envolvidos na organização de eventos e na organização ou apoio a atividades turísticas (um exemplo sendo o ciclo de Mega Eventos sediados pelo Brasil desde 2012). Os casos reportados ressaltam, em grande parte, o investimento do setor em tecnologias de vigilância para garantir a segurança desses espaços/eventos. O principal uso dessas tecnologias é paramonitorar o fluxo de pessoas e garantir o videomonitoramento contínuo desses espaços.

O setor representa 3% dos casos mapeados no Brasil (ver gráfico 1). Os casos concentram- se nos anos de 2014 a 2016 e, posteriormente, de 2019 a 2020, uma vez que nesses respectivos períodos houve um crescimento de tecnologias de vigilância com intuito de apoiar a segurança de megaeventos, como a Copa do Mundo (2014), Olimpíadas (2016) e Copa América no Brasil (2019).

Videomonitoramento é a segunda maior categoria mapeada, com 25% dos casos[69], fazendo com que, desses 87,5% sejam relacionados a dados de imagem[70]. Principais exemplos de casos mapeados:

- **COPA DO MUNDO 2014**: A partir da Secretaria Extraordinária de Segurança para Grandes Eventos, do Ministério da Justiça e Segurança Pública, foram adquiridas câmeras de videomonitoramento para a Copa do Mundo 2014, na cidade do Rio de Janeiro.

- **JOGOS OLÍMPICOS 2016**: Em ações de policiamento durante as Olimpíadas 2016, na cidade do Rio de Janeiro, foram utilizados balões com câmeras de alta resolução. Tecnicamente chamados de "aeróstatos de monitoramento persistente de grandes áreas", os mesmos enviavam imagem, em tempo real, para os centros de Comando e Controle[71].

68 Venturini, 2019 / Valderrama, 2021

69 No caso do setor de Eventos/Turismo, no Brasil, os casos levam a universo de 12 classificações de funcionalidades.

70 No caso do setor de Eventos/Turismo, no Brasil, os casos levaram a um universo de 8 classificações de tipos de dados mapeados pelo setor.

71 Agência Brasil (2015). Balões com câmeras vão auxiliar ações de segurança durante Olimpíada 2016. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2015-10/policia-do-rio-tera-baloes-com-cameras-para-auxiliar-acoes-durante-olimpiada

Conclusão

A análise do panorama da implementação de tecnologias de vigilância no Brasil e na América Latina revela um cenário preocupante. Observamos a vasta aplicação de tecnologias na segurança pública e no setor de saúde. Também identificamos uma concentração e normalização de processos de captura de imagens e de dados biométricos como pilares para o funcionamento de uma infraestrutura de monitoramento pelo Estado. O setor de saúde, por exemplo, se destaca por ser o setor que coleta a maior variedade de dados. Práticas corriqueiras de coleta de dados vão desde medições biométricas para avaliar se passantes estão ou não como máscaras, até a coleta de dados sensíveis de saúde dos usuários que buscam aplicativos de rastreamento de contato. Se antes não havia grande uso de tecnologia de vigilância por parte do poder público nessa área, a Covid 19 claramente mudou o cenário. Cooperação entre iniciativa privada e poder público ajudou a impulsionar os diferentes usos, incluindo o desenvolvimento de aplicativos para o controle de contato, monitoramento de sintomas, telemedicina e entre outros.

O mapeamento mostrou ainda como a prática de vigilância alcança outros setores como economia, educação, turismo e inteligência. Mesmo que o número de casos nesses outros setores não seja tão expressivo como em Segurança Pública — seja pela falta de informações e cobertura de imprensa, pela maior presença de atores privados na sua implementação ou pela falta de transparência no que tange às aquisições destas ferramentas — a pesquisa revela que a implementação de tecnologias de vigilância é uma tendência que ganha maior tração após 2020.

O objetivo do relatório é proporcionar uma visão sobre como cada setor utiliza esses projetos, suas particularidades em termos de coleta de dados, implementadores e tecnologias. Essa visão intersetorial poderá fomentar o debate público sobre vigilância e implementação de tecnologias, uma vez que questiona tanto o Estado, quanto o vigilantismo enquanto algo único e coeso. Pelo contrário, compreendemos que o amadurecimento do debate público se expressa no detalhamento da discussão sobre riscos associados com a aquisição e implementação de tecnologias de monitoramento. Para isso, precisamos estar equipados com entendimento sobre as características específicas do vigilantismo em cada setor. Contudo, conforme mencionado anteriormente, o presente relatório não é exaustivo no que diz respeito ao número de casos mapeados. Entretanto, vemos que esse relatório é um primeiro passo para novas perguntas de pesquisa e de incidência, as quais incluem, mas não se restringem, ao desenvolvimento e aprimoramento de metodologias para o estudo do vigilantismo por meio da implementação de uma tipologia que possa auxiliar na catalogação e acompanhamento sistemático de casos reportados. Esperamos que, assim como nos ajudou no levantamento de 300 casos, esta Tipologia possaservir como instrumento para outras organizações continuarem com o esforço de fomentar o debate público intersetorial com pesquisas baseadas em evidências. E que as mesmas possam trazer luz sobre a problemática realidade do vigilantismo a partir de uma visão da América Latina e do Brasil.

Anexo 1: Tipologia

Os casos mapeados pela pesquisa foram classificados de acordo com a tipologia a seguir. A tipologia é composta por uma classificação que permite o mapeamento sistemático da implementação de tecnologias de vigilância pelo Estado. Desenvolvemos um framework analítico com três dimensões: principal funcionalidade da tecnologia, componentes tecnológicos e implementação. Além disso, a tipologia contém os setores que implementaram as tecnologias[72].

TABELA 2: Tipologia para analisar a implementação de tecnologias de vigilância pelo Estado

Setores	Funcionalidade da tecnologia	Componentes tecnológicos	Implementação
• Economia • Educação • Inteligência • Saúde • Segurança Pública • Transporte • Eventos/ Turismo	*Aplicativos[73] *Câmeras Corporais *Drones *Integração de bases de dados *Interceptação comunicacional *Monitoramento de fluxos de pessoas e objetos *Monitoramento geoespacial *Monitoramento informacional e/ou comunicacional *Monitoramento de temperatura *Predição *Reconhecimento Facial *Reconhecimento de Placas *Spyware *Videomonitoramento	**Fonte de dados** *GPS *Bluetooth *Redes Sociais *Sensores *Terceiros *Hardware *Indivíduo **Tipo de dado coletado** *Dados anonimizados *Dados de imagem *Dados pessoais *Dados biométricos *Dados sensíveis *Dados de geolocalização	**Desenvolvedor** *Cooperação Público-Privada *Setor público *Setor privado *Não informado **Principal implementador** *Agências de Inteligência *Empresas *Forças Armadas *Governos locais *Ministérios *Polícia *Não informado

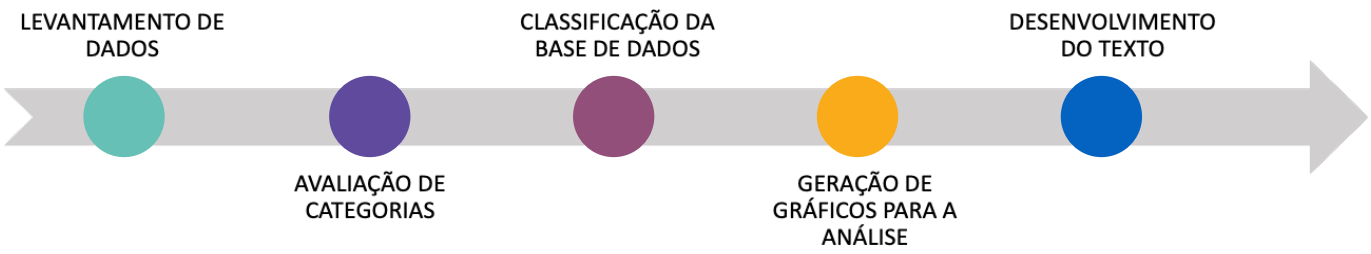
72 Instituto Igarapé (2022). Uma tipologia para analisar a implementação de tecnologias de vigilância pelo Estado. Disponível em: LINK

73 Foi feita a leitura da política de uso e privacidade de alguns dos aplicativos mapeados, bem como o seu uso, para um melhor entendimento do funcionamento de cada um e da forma de coleta de dados. Exemplos de aplicativos testados foram: “Be On”, “Monitora Covid”, “Dados do Bem”.

Anexo 2: Metodologia

Ao longo de 2020 e 2021, coletamos 300 casos de implementação de tecnologias de vigilância no Brasil e em outros países na América Latina. O processo de pesquisa foi dividido em diversas etapas que, por vezes, foram realizadas de forma concomitante e combinando uma abordagem qualitativa e quantitativa:

Figura 1: Etapas e desenho de pesquisa



LEVANTAMENTO DE DADOS: Na primeira fase da pesquisa, realizamos uma revisão de literatura sobre o emprego de tecnologias de vigilância nos países do Sul Global, na América Latina e no Brasil, mais especificamente. A pesquisa de fontes secundárias contou com relatórios, artigos, livros, fontes midiáticas, entre outros. Com base nessa revisão, identificamos a primeira leva de casos publicamente reportados. Em seguida, realizamos um levantamento de fontes primárias por meio de busca em portais de transparência e acesso à informação (no Brasil) como TCU, portais estaduais de compras, entre outros, focando tanto na identificação de dados complementares aos casos já então mapeados, bem como realizando novas buscas por projetos implementados pelos diferentes estados no país. Deseja-se registrar, porém, que os portais apresentaram constantes instabilidades ou troca de endereços eletrônicos de determinadas páginas, o que demonstra certa limitação para fins de pesquisa de transparência no Brasil.

AVALIAÇÃO DE CATEGORIAS: Ao longo do levantamento de casos, buscamos identificar padrões nas práticas de implementação, tecnologias predominantes e principais atores envolvidos. No primeiro momento, trabalhamos com uma abordagem indutiva de levantamento de categorias para a estrutura da tipologia. Realizamos três rodadas de discussões em um exercício de mapa mental dos casos mapeados, separando as tendências identificadas que apresentavam maior consistência no contexto dos dados coletados. Em um segundo momento, e após um exercício inicial de classificação dos casos, reavaliamos, a partir de uma abordagem dedutiva, a estrutura das categorias priorizando a divisão setorial como eixo norteador da análise.

CLASSIFICAÇÃO DA BASE DE DADOS: No processo de classificação dos dados a partir das categorias da tipologia, decidimos atribuir mais de uma classificação para "funcionalidade da tecnologia" e "componentes tecnológicos" (fontes de dados e tipos de dados). Dessa forma, foi possível observar e traçar as múltiplas funções que um projeto de vigilância costuma ter no contexto de sua implementação.

GERAÇÃO DE GRÁFICOS PARA A ANÁLISE: Para melhor retratar a complexidade e diversidade de práticas de vigilância sendo empregadas pelo setor público, decidimos priorizar a divisão setorial como eixo principal da pesquisa. Dessa forma, a distribuição de tecnologias, bem como dos atores envolvidos no fornecimento e distribuição de sistemas, softwares e dispositivos, contaram com uma visão não só geográfica (estados e países na América Latina) mas também com nuances de sua implementação no contexto da segurança pública, saúde e entre outros.

DESENVOLVIMENTO DO TEXTO: Por fim, o desenvolvimento da análise dos dados no relatório presente contou com um retorno ao material qualitativo (descrição dos casos e revisão de literatura), que foi combinado com a análise estatística.

Referências

ABDI (2021). Fronteira Tech. Disponível em: https://www.abdi.com.br/projetos/fronteira-tech

Access Now (2021). Surveillance Tech in Latin America: Made Abroad, Deployed at Home. Disponível em https://www.accessnow.org/cms/assets/uploads/2021/08/Surveillance-Tech-Latam-Report.pdf

Acha, Gisela Pérez de (2016) in Hacking Team Malware para la Vigilancia en América Latina. Disponível em https://www.derechosdigitales.org/wp-content/uploads/malware-para-la-vigilancia.pdf

Agência Brasil (2015). Balões com câmeras vão auxiliar ações de segurança durante Olimpíada 2016. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2015-10/policia-do-rio-tera-baloes-com-cameras-para-auxiliar-acoes-durante-olimpiada

Arroyo, Verónica in Access Now (2020). Tecnologías de vigilancia para controlar el COVID-19 en América Latina. Disponível em https://www.accessnow.org/tecnologias-de-vigilancia-para-controlar-el-covid-19-en-america-latina/

BBC (2021). Pegasus: o que é o sistema que espionou jornalistas, ativistas e advogados. Disponível em: https://www.bbc.com/portuguese/internacional-57885795

Bruno Ribeiro. (2017). Doações de chineses a Doria somam R$ 8,5 mi. Disponível em: https://sao-paulo.estadao.com.br/noticias/geral,doacoes-de-chineses-a-sp-somam-r-8-5-mi,70001912058

Byrne, J. & Marx, G. (2011). Technological Innovations in Crime Prevention and Policing. A Review of the Research on Implementation and Impact. Disponível em https://www.ojp.gov/pdffiles1/nij/238011.pdf

Carta Capital (2022). De Oakland ao Jacarezinho: os sistemas de reconhecimento facial precisam ser banidos. Disponível em: https://www.cartacapital.com.br/blogs/de-oakland-ao-jacarezinho-os-sistemas-de-reconhecimento-facial-precisam-ser-banidos/#:~:text=A%20legisla%C3%A7%C3%A3o%20federal%20nos%20Estados,em%20seguida%2C%20Oakland%2C%20tamb%C3%A9m%20na

Clarke et al. Biomedicalization: Technoscience, Health, and Illness in the U.S (2010). Disponível em: https://www.degruyter.com/document/doi/10.1515/9780822391258/html

Crypto ID (2021).Governo Federal testa Embarque + Seguro no Aeroporto de Brasília. Disponível em https://cryptoid.com.br/governo-digital-government/governo-federal-testa-embarque-seguro-no-aeroporto-de-brasilia/

ECOSOC Resolution 2002/13. Annex: Guidelines for the Prevention of Crime. Disponível em https://www.unodc.org/documents/justice-and-prison-reform/crimeprevention/resolution_2002-13.pdf

El País (2019). Vírus para espionagem política denunciado pelo WhatsApp foi usado no Brasil. Disponível em: https://brasil.elpais.com/brasil/2019/05/15/tecnologia/1557877977_241967.html

Extra (2020). Em Bogotá, polícia colombiana usa drones para detectar temperatura e aglomeração. Disponível em https://extra.globo.com/noticias/mundo/em-bogota-policia-colombiana-usa-drones-para-detectar-temperatura-aglomeracao-rv1-1-24437102.html

Folha de São Paulo (2019). Reconhecimento facial bloqueia 331 mil Bilhetes Únicos em SP: Tecnologia foi instalada nas catracas para evitar fraudes. Disponível em https://agora.folha.uol.com.br/sao-paulo/2019/06/reconhecimento-facial-bloqueia-331-mil-bilhetes-unicos-em-sp.shtml

Feldstein, Steven (2019): The Global Expansion of AI Surveillance. Disponível em: https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf

Frost & Sullivan (2016). Tornando as Cidades Inteligentes mais seguras: Uma Perspectiva Latino Americana. Disponível em: https://br.nec.com/pt_BR/safety/pdf/wp_safercities.pdf

G1 (2020). Governo de SP instala câmera que mede temperatura e detecta uso de máscara na estação Sé do Metrô. Disponível em: https://g1.globo.com/sp/sao-paulo/noticia/2020/07/02/governo-de-sp-instala-camera-que-mede-temperatura-e-detecta-uso-de-mascara-em-estacao-de-se-do-metro.ghtml

Gobernación Valle Del Cauca (2020). Los vallecaucanos cuentan con 'CaliValleCorona', la App que les permitirá realizar una autoevaluación sobre Covid-19. Disponível em: https://www.valledelcauca.gov.co/publicaciones/65721/los-vallecaucanos-cuentan-con-calivallecorona-la-app-que--les-permitira-realizar-una-autoevaluacion-sobre-covid-19/

Gomes, Mariana (2021) in Le Monde Diplomatique Brasil. A naturalização de sistemas e tecnologias de vigilância na pandemia. Disponível em: https://diplomatique.org.br/a-naturalizacao-de-sistemas-e-tecnologias-de-vigilancia-na-pandemia/

Governo da Bahia (2021). Salvador e mais 77 municípios contarão com ampliação de serviço de reconhecimento facial e de placas. Disponível em: http://www.bahia.ba.gov.br/2021/07/noticias/salvador-e-mais-77-municipios-contarao-com-ampliacao-de-servico-de-reconhecimento-facial-e-de-placas/?amp

Governo de São Paulo (2020). Isolamento Social em São Paulo é de 49% aponta sistema de monitoramento inteligente. Disponível em: https://www.desenvolvimentoeconomico.sp.gov.br/isolamento-social-em-sao-paulo-e-de-49-aponta-sistema-de-monitoramento-inteligente-2/

Grabosky, P. (1998). Technology and Crime Control. Australian Institute of Criminology. Disponível em https://www.aic.gov.au/sites/default/files/2020-05/tandi078.pdf

Haggerty, K.; Wilson, D.; Smith, G.J.D. (2011). Theorizing Surveillance in Crime Control. Disponível em https://journals.sagepub.com/doi/pdf/10.1177/1362480610396442

Hurel et al. in El País (2021). Pegasus, a ponta do iceberg da fragilidade no controle de inteligência e uso de tecnologias de vigilância. Disponível em: https://brasil.elpais.com/opiniao/2021-08-02/pegasus-a-ponta-do-iceberg-da-fragilidade-no-controle-de-atividades-de-inteligencia-e-uso-de-tecnologias-de-vigilancia.html?event_log=fa

IDEC (2021). ViaQuatro é condenada por reconhecimento facial no Metrô de SP. Disponível em: https://idec.org.br/idec-na-imprensa/viaquatro-e-condenada-por-reconhecimento-facial-sem-autorizacao-no-metro-de-sp

Instituto Igarapé (2022). Uma tipologia para analisar a implementação de tecnologias de vigilância pelo Estado. Disponível em: LINK

Instituto Igarapé (2020). Reconhecimento Facial no Brasil. Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/

Kurtz, Lahis in IRIS (2019). Vigilância é uma solução ou uma ameaça à segurança pública?. Disponível em https://irisbh.com.br/vigilancia-e-uma-solucao-ou-uma-ameaca-a-seguranca-publica/

Lobo, Renato in Viatrolebus (2021). Equipamento mede temperatura e uso de máscara em estações de trens argentinas. Disponível em: https://viatrolebus.com.br/2021/02/equipamento-mede-temperatura-e-uso-de-mascara-em-estacoes-de-trens-argentinas/

López, Joan. The Case of the Solidarity Income in Colombia:The Experimentation With Data on Social Policy During the Pandemic In COVID-19 from the Margins: Pandemic invisibilities, Policies and Resistance in the Datafied Society. Milan, S.; Treré, E.; Masiero, S. (edit). Theory on Demand #40. Amsterdam, Institute of Network Cultures, 2021 pp.126 - 128

Lupton, Deborah (2014). "Apps as Artefacts: Towards a Critical Perspective on Mobile Health and Medical Apps" in Societies 4, no. 4: 606-622. Disponível em: https://doi.org/10.3390/soc4040606

Marczak et al. (2018). Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries. Disponível em: https://tspace.library.utoronto.ca/bitstream/1807/95391/1/Report%23113--hide%20and%20seek.pdf

NEC (2015). NEC to provide facial recognition systems for 14 international airports in Brazil. Disponível em https://www.nec.com/en/press/201507/global_20150716_02.html

OECD (2020). Latin American Economic Outlook 2020 : Digital Transformation for Building Back Better. Disponível em: https://www.oecd-ilibrary.org/sites/e7a00fd6-en/index.html?itemId=/content/component/e7a00fd6-en

OHCHR Resolution; (2019) A/HRC/41/35. Surveillance and human rights - Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. Disponível em: https://www.ohchr.org/en/documents/thematic-reports/surveillance-and-human-rights-report-special-rapporteur-promotion-and

Olhar Digital (2020). Covid 19: Prefeitura do Rio usa drone 'falante' contra aglomeração. Disponível em: https://olhardigital.com.br/2020/04/15/coronavirus/covid-19-prefeitura-do-rio-usa-drone-falante-contra-aglomeracoes/

Prefeitura de Erechim (2021). Projeto Sentinela Reforça Segurança dos Erechinenses. Disponívle em: https://www.pmerechim.rs.gov.br/noticia/15398/13-07-2021/projeto-sentinela-reforca-seguranca-dos-erechinenses

Prefeitura de Recife (2020). Prefeitura do Recife usa tecnologia como aliada na contenção do novo coronavírus. Disponível em: http://www2.recife.pe.gov.br/noticias/24/03/2020/prefeitura-do-recife-usa-tecnologia-como-aliada-na-contencao-do-novo-coronavirus

_____ (2020). Recife incorpora uso de drones para ampliar índice de isolamento social. Disponível em http://www2.recife.pe.gov.br/noticias/17/04/2020/recife-incorpora-uso-de-drones-para-ampliar-indice-de-isolamento-socialc

Salvo, Philip Di. Solutionism, Surveillance, Borders and Infrastructures in the "Datafied Pandemic". In COVID-19 from the Margins: Pandemic invisibilities, Policies and Resistance in the Datafied Society. Milan, S.; Treré, E.; Masiero, S. (edit). Theory on Demand #40. Amsterdam, Institute of Network Cultures, 2021 pp. 164 - 170.

The Intercept (2021). Lentes Racistas: “Rui Castro está transformando a Bahia em um laboratório de vigilância com reconhecimento facial”. Disponível em: https://theintercept.com/2021/09/20/rui-costa-esta-transformando-a-bahia-em-um-laboratorio-de-vigilancia-com-reconhecimento-facial/

_____ (2020). Da placa do Carro ao CPF: Conheça o Cortex, Sistema de Vigilância do Governo que integra placa de carro dados de emprego. Disponível em: https://theintercept.com/2020/09/21/governo-vigilancia-cortex/

Tudo Celular.com (2020). Coronavírus: Movimento Brasil Sem Corona ajuda prefeitura pernambucana a combater a doença. Disponível em https://www.tudocelular.com/tech/noticias/n158068/brasil-sem-corona-ajuda-prefeitura-identificacao.html

UOL (2020). Relatório do governo separa em grupos jornalistas e influenciadores. Disponível em: https://noticias.uol.com.br/colunas/rubens-valente/2020/12/01/governo-bolsonaro-jornalistas-redes-sociais.htm

____ (2021). Além do Pegasus, Carlos Bolsonaro queria sistema para monitorar o Planalto. Disponível em: https://noticias.uol.com.br/politica/ultimas-noticias/2021/08/03/alem-do-pegasus-carlos-bolsonaro-previa-sistema-para-monitorar-planalto.htm

Valderrama, Matías (2021). Sistema Alerta Niñez e la predicción del riesgo de vulneración de derechos de la infancia. Disponível em: https://ia.derechosdigitales.org/wp-content/uploads/2021/03/CPC_informe_Chile.pdf

Venturini, Jamila in Derechos Digitales (2019). Vigilância, controle social e desigualdade: a tecnologia reforça vulnerabilidades estruturais na América Latina. Disponível em: https://www.derechosdigitales.org/13921/vigilancia-controle-social-e-desigualdade-a-tecnologia-reforca-vulnerabilidades-estruturais-na-america-latina/

Venturini & Souza (2020): Tecnologias e Covid-19 no Brasil: vigilância e desigualdade social na periferia do capitalismo. Disponível em: https://br.boell.org/sites/default/files/2020-06/Tecnologias%20e%20Covid-19%20no%20Brasil%20vigil%C3%A2ncia%20e%20desigualdade%20social%20na%20periferia%20do%20capitalismo.pdf

Leia também

E CONHEÇA
Portal Brasileiro
da Cibersegurança

Metodologia para analisar a implementação de tecnologias de vigilância pelo estado
(Outubro 2022)

CIBERSEGURANÇA NO BRASIL: uma análise da estratégia nacional
Louise Marie Hurel.
(Abril 2021)

REGULAÇÃO DO RECONHECIMENTO FACIAL NO SETOR PÚBLICO
Pedro Augusto P. Francisco, Louise Marie Hurel e Mariana Marques Rielli**.**
(Junho 2020)

INSTITUTO IGARAPÉ
a think and do tank

O Instituto Igarapé é um think and do tank independente, dedicado à integração das agendas de segurança, clima e desenvolvimento. Nosso objetivo é propor soluções e parcerias a desafios globais por meio de pesquisas, novas tecnologias, influência em políticas públicas e comunicação. Somos uma instituição sem fins lucrativos, independente e apartidária, com sede no Rio de Janeiro, mas cuja atuação transcende fronteiras locais, nacionais e regionais. Premiada como a melhor ONG de Direitos Humanos no ano de 2018, o melhor think tank em política social pela Prospect Magazine em 2019 e considerada pelo Instituto Doar, pelo segundo ano consecutivo, como uma das 100 melhores organizações brasileiras do terceiro setor.

O programa de Segurança Digital do Instituto Igarapé se dedica ao desenvolvimento de pesquisas interdisciplinares, facilitação de diálogos intersetoriais e promoção de espaços de confiança e conscientização para o avanço de políticas digitais. Trabalhamos com temas como segurança digital, crimes na Internet, inteligência artificial, Internet das coisas, proteção de dados e cidades inteligentes. Construímos plataformas, pensamos criticamente sobre o impacto dessas tecnologias na sociedade e trabalhamos para abordar os desafios à proteção de direitos digitais mediante o avanço da implementação de tecnologias em nosso dia a dia. **igarape.org.br/temas/seguranca-digital**

Instituto Igarapé

Rio de Janeiro - RJ - Brasil
Tel/Fax: +55 (21) 3496-2114
contato@igarape.org.br
facebook.com/institutoigarape
twitter.com/igarape_org
instagram.com/igarape_org/

igarape.org.br

Direção Criativa
Raphael Durão - STORMdesign.com.br

ISSN 2359-0998

igarape.org.br

INSTITUTO IGARAPÉ
a think and do tank