

Tecnologias disruptivas em segurança pública: uma análise situacional brasileira

RESUMO

Este artigo investiga o uso de tecnologias disruptivas, como Inteligência Artificial, Big Data, Machine Learning e Internet das Coisas, como ferramentas de apoio às atividades de segurança pública nas 27 Unidades da Federação (UFs) no Brasil. Além disso, o estudo avalia a divulgação de dados e informações pelas instituições de segurança pública estaduais para pesquisadores, bem como o prazo de retorno das respostas. Por meio da pesquisa foi possível obter informações sobre a adoção dessas tecnologias e apontar alguns desafios enfrentados. Os resultados revelam que seis estados (22,22%) adotam – pelo menos uma – das tecnologias pesquisadas, enquanto quatro (14,81%) mencionaram iniciativas de adoção. Por outro lado, 12 estados (44,44%) afirmaram não utilizar as referidas tecnologias e outros 9 (33,33%) não responderam aos questionamentos. A pesquisa destaca a importância das parcerias entre instituições de ensino e instituições de segurança pública, além da padronização nacional e compartilhamento de dados atualizados para pesquisa e análise.

PALAVRAS-CHAVE: Inteligência artificial. Big data. Internet das coisas. Machine learning. Disruptiva.

Denise Fukumi Tsunoda
Universidade Federal do Paraná,
Curitiba, Paraná, Brasil
dtsunoda@ufpr.br

Ana Clara Cândido
Universidade Federal de Santa
Catarina, Florianópolis, Santa
Catarina, Brasil
ana.candido@ufsc.br

André José Ribeiro Guimarães
Universidade Federal do Paraná,
Curitiba, Paraná, Brasil
andrejose@ufpr.br

INTRODUÇÃO

O Global Peace Index (GPI) (INSTITUTE FOR ECONOMICS & PEACE, 2023), elaborado pelo Institute for Economics and Peace (IEP), é reconhecido como a principal métrica para avaliar a paz global. O relatório divulgado em junho de 2023 apresenta uma abrangente análise baseada em dados sobre “tendências da paz, seu valor econômico e como desenvolver sociedades pacíficas”. O GPI é calculado com base em 23 indicadores qualitativos e quantitativos e mede o estado de paz em três domínios: o nível de segurança e proteção social, a extensão do conflito doméstico e internacional em andamento e o grau de militarização.

Nessa edição, o Brasil ocupa a 132ª posição entre os 163 países avaliados. Se considerada apenas a América do Sul, o Brasil está em 9º lugar entre os 11 países analisados pelo IEP (com exceção do Suriname, que não foi mencionado), sendo classificado como um país com um índice de paz superior apenas ao da Venezuela e da Colômbia. O índice Estado de Paz é categorizado em níveis como “muito alto”, “alto”, “médio”, “baixo”, “muito baixo” e “não incluído”. O Brasil encontra-se na categoria “baixo”, assim como Estados Unidos, Líbia, México, Palestina, Paquistão, Etiópia, Israel e outros países. Por outro lado, está em uma categoria melhor que Iraque, Rússia, Afeganistão, Síria e outros. O relatório aponta que o GPI teve um aumento quase contínuo de 2009 a 2019, em grande parte devido ao “grande desenvolvimento tecnológico e desenvolvimento econômico” dos países.

O Instituto de Pesquisa Econômica e Aplicada (IPEA) publicou em 2015 um material com o título “Violência e segurança pública em 2023: cenários exploratórios e planejamento prospectivo” (FERREIRA; MARCIAL, 2015). Esse documento foi elaborado pelo próprio IPEA em parceria com a Secretaria de Assuntos Estratégicos da Presidência da República (SAE/PR), o Ministério da Justiça e o Ministério do Planejamento, Orçamento e Gestão (MP). Nele, os autores apresentaram cenários, 44 tendências e 8 incertezas-chave. As incertezas poderiam alterar o rumo dos acontecimentos, mas foram propostos 12 objetivos estratégicos, dentre os quais, dois (página 120) estão relacionados à pesquisa em pauta: “Fortalecer investimentos em inteligência e perícia, com uso de novas tecnologias, para melhorar a capacidade resolutive.” e o “Consolidar sistemas de informação, com produção e monitoramento de indicadores, como forma de balizar a elaboração de políticas, melhorar a gestão e produzir diagnósticos.”. No entanto, o documento não especifica quais tecnologias potenciais seriam essas.

No mesmo material de 2015 (FERREIRA; MARCIAL, 2015), algumas possíveis aplicações de tecnologia são apresentadas como cenários em 2023:

- a) crescimento da difusão de inovações tecnológicas nas áreas de segurança pública e privada: a expansão da segurança privada, associada às compras públicas, tem levado a uma maior inovação e difusão de tecnologias para fins de segurança. Um exemplo citado é o aumento na utilização de câmeras de segurança. Com o avanço tecnológico e o crescimento do consumo de novos produtos, espera-se um crescimento da difusão de inovações tecnológicas nas áreas de segurança pública e privada (página 71);
- b) programa Corujão: programa que envolve fiscalização de bares e casas noturnas em bairros com alta taxa de homicídios (página 98);

- c) Furto Zero: acordo do Ministério da Justiça com empresas de telefonia para o travamento de celulares subtraídos, e com a indústria e oficinas automobilísticas para a gravação de chassi nas peças (página 98);
- d) programa Big Brother: instalação de câmeras de vigilância, pelas prefeituras, em áreas de maior circulação e iluminação em locais ermos (página 98);
- e) qualificação policial: a Secretaria Nacional de Segurança Pública (Senasp) tem fortalecido os programas de qualificação policial (investigação, gestão, polícia cidadã), o desenvolvimento de sistemas de informação e monitoramento, e a utilização de inovações tecnológicas (página 98). Esses três pontos têm contribuído para o aumento da efetividade da investigação criminal e implantação pelos governos estaduais de delegacias especializadas nas cidades mais populosas para crimes violentos (homicídio, sequestro, roubo, estupro).

Alguns destes cenários são discutidos nesta pesquisa realizada em 2023 junto às unidades de segurança pública de todas as unidades federativas do país, com o objetivo de identificar o uso de tecnologias disruptivas na área de segurança pública.

Embora a origem do termo “tecnologia disruptiva” não seja atribuída a uma única pessoa, Clayton M. Christensen, ex-professor de Harvard, é reconhecido como o autor que popularizou e explorou o conceito na obra de 1997 “The Innovator's Dilemma”, publicado no Brasil como O Dilema da Inovação (CHRISTENSEN, 2012).

Uma tecnologia disruptiva pode ser definida como uma inovação que altera significativamente um mercado ou setor, rompendo com os modelos de negócios existentes e transformando a forma como as coisas são feitas. Essas tecnologias têm o potencial de causar impactos significativos em diversos setores, impulsionando mudanças e proporcionando avanços (ou não) substanciais. Christensen (2012) argumenta que as empresas líderes tendem a se concentrar em melhorar seus produtos e serviços existentes, ignorando inovações aparentemente menos sofisticadas ou de menor qualidade que, ao longo do tempo, podem ganhar mercado e se tornar uma ameaça aos negócios estabelecidos. E complementa que a “proteção mais poderosa” das pequenas empresas desfrutam é que enquanto criam mercados emergentes para tecnologias de ruptura, estão “fazendo algo que as líderes tradicionais simplesmente não veem sentido em fazer”.

A aplicação de tecnologias disruptivas é fundamental para modernização e transformação do setor de segurança pública por facilitar o enfrentamento das violências por meio tanto da prevenção e quanto do combate ao crime. A ciência e a tecnologia são moldadas e influenciadas pelo contexto social, econômico e político. As demandas da sociedade por maior segurança e eficiência na aplicação da lei impulsionam a pesquisa e o desenvolvimento de tecnologias disruptivas em segurança pública. O uso dessas tecnologias tem implicações profundas na sociedade, com destaque para as melhorias na capacidade da aplicação da lei na prevenção de crimes e resposta rápida a emergências; por outro lado, suscita preocupações com a privacidade e a ética, considerando-se que o aumento da vigilância e da coleta de dados levanta questões sobre privacidade e o uso ético das informações pessoais. Na mesma linha, é necessária atenção para que os

vieses algorítmicos sejam suprimidos para garantir que as tecnologias sejam aplicadas de maneira equitativa e transparente, sem criar ou reforçar disparidades sociais (OLIVEIRA et al., 2022; VIEIRA, 2019).

Dentre as diversas tecnologias, um levantamento realizado em 2022 (TSUNODA, CÂNDIDO, 2022) apontou quatro em destaque: Inteligência Artificial, Machine Learning, Internet das Coisas e Big Data. Ainda que Machine Learning (ML) tenha estreita relação com inteligência artificial, nesta pesquisa serão consideradas como tecnologias distintas.

A Inteligência Artificial (IA) tem sido amplamente empregada na segurança pública para diversas finalidades. Essas aplicações incluem emissão de multas em veículos com excesso de velocidade, monitoramento de paradas em faixas de pedestres, identificação de comportamentos suspeitos e ou agressivos, detecção de ameaças em vídeos e imagens estáticas, determinação de áreas de maior risco e capacidade de análise em tempo real de grandes volumes de dados para aprimorar a inteligência policial.

Enquanto a IA abrange uma ampla gama de métodos e abordagens para imitar a inteligência humana, o ML se concentra no desenvolvimento de algoritmos e modelos capazes de aprender e tomar decisões com base em dados e permite que os sistemas aprendam e melhorem com base nos dados, sem a necessidade de programação específica para cada situação. Na área de segurança pública, o ML pode ser utilizado na identificação de padrões, como reconhecimento facial e rastreamento de veículos e indivíduos. Também pode ser aplicado na prevenção de eventos, como comportamentos suspeitos em eventos públicos, por exemplo. Além disso, o ML auxilia na tomada de decisões com base em análises de dados, como detecção de fraudes para prevenção de crimes de lavagem de dinheiro e fraude eletrônica, além de ajudar a prevenir congestionamentos e outros desafios.

Outra tecnologia disruptiva é a Internet das Coisas (IoT), que possibilita a interconexão de dispositivos e sistemas de segurança. Na área de segurança pública, a IoT permite, por exemplo, o monitoramento de áreas públicas para identificar movimentos suspeitos e acionar alertas automáticos com o uso de sensores e câmeras inteligentes. Igualmente, é comum o uso de drones em operações de vigilância, busca e salvamento, e até mesmo no monitoramento de fronteiras.

A quarta tecnologia disruptiva pesquisada é o Big Data, que se refere à capacidade de coletar, armazenar e analisar grandes volumes de dados provenientes de diversas fontes, como redes sociais, documentos diversos, câmeras de segurança, entre outros. A diversidade e quantidade de dados permite a identificação de padrões comportamentais, antecipação de possíveis ameaças, conexões em análises de dados forenses, maior velocidade nas investigações e insights que, muitas vezes, poderiam passar despercebidos pelos policiais.

Segundo Silva e Limeira (2023), a era da sociedade em rede apresenta diversidade de implicações ligadas à gestão e proteção dos dados e os riscos associados ao “uso inadequado” e à divulgação de dados e informações pessoais são inúmeros. Por outro lado, os autores concluem na pesquisa que as tecnologias inovadoras de manipulação dos dados (mesmo os pessoais) oferecem inúmeras vantagens em vários aspectos da vida em comunidade.

Desta forma, o objetivo desta pesquisa é verificar o uso de tecnologias disruptivas tais como: Inteligência Artificial, Big Data, Machine Learning e Internet das Coisas como suporte às atividades de segurança pública nas 27 Unidades da Federação do Brasil, que englobam os 26 estados e o Distrito Federal. De forma complementar, a pesquisa avalia como as UFs disponibilizam os dados e informações para os pesquisadores, considerando o tempo e qualidade das respostas fornecidas.

METODOLOGIA

Inicialmente, com o objetivo de identificar a adoção de Inteligência Artificial e demais tecnologias disruptivas, de acordo com a análise da produção científica mundial de Tsunoda e Cândido (2022), em 23 de janeiro de 2023, todas as 27 Unidades da Federação (UFs) - 26 estados e Distrito Federal – foram contatadas via e-mail. A mensagem continha os seguintes tópicos:

- a) consultar sobre a adoção de alguma tecnologia de Inteligência Artificial nos seus procedimentos (podendo ser para análise de dados, reconhecimento de imagens ou qualquer outro propósito);
- b) verificar se as seguintes tecnologias são utilizadas para algum propósito: Big Data, IoT e Machine Learning.

Foram enviados novos e-mails em 08 de maio e 19 de junho de 2023 para as instituições de segurança pública que não forneceram respostas anteriormente.

Foi constatada a ausência de padronização na solicitação de informações junto às unidades de segurança pública estaduais e do Distrito Federal. Embora o mesmo e-mail tenha sido enviado a todas as unidades da federação, conforme cadastrado junto ao Ministério da Justiça, não houve uma orientação uniforme sobre como a solicitação deveria ser encaminhada em cada UF. Entre as diferentes instruções recebidas, destacam-se:

- a) sugestão de abertura de solicitação em sistema específico para solicitação de informações, conforme Lei de Acesso à Informação;
- b) recomendação de que as informações fossem solicitadas junto às ouvidorias estaduais;
- c) direcionamento da demanda para às delegacias de polícia civil;
- d) negativa de qualquer resposta com a justificativa de que não podem fornecer dados sensíveis, em atendimento à LGPD;
- e) exigência de cadastro da demanda no Fala.BR;
- f) redirecionamento do e-mail para outras unidades.

Apenas para fins de esclarecimento, as questões propostas não demandam, de forma alguma, o fornecimento de dados sensíveis ou sujeitos à proteção da Lei Geral de Proteção de Dados Pessoais (LGPD). No entanto, apesar das tentativas de argumentação, alguns estados negaram as respostas se valendo desta justificativa.

Faz mister mencionar que o “Enunciado CGU nº 11/2023 - Restrições de acesso em virtude da desarrazoabilidade ou desproporcionalidade do pedido” menciona que pedidos de acesso à informação somente podem ser negados sob o

fundamento da "desarrazoabilidade" se o órgão ou entidade pública demonstrar haver risco concreto associado à divulgação da informação; e, por sua vez, sob o fundamento da "desproporcionalidade" se o órgão evidenciar não possuir recursos, humanos ou tecnológicos, para atender o pedido. Para as duas situações, não podem tais argumentos serem utilizados como fundamento geral e abstrato para a negativa de acesso. Além disso, quando restar configurada a desproporcionalidade do pedido, o órgão ou entidade deve disponibilizar os meios para que o cidadão realize a consulta *in loco*, para efetuar a reprodução ou obter os documentos desejados, em conformidade com o disposto no art. 11, §1º, I, da Lei nº 12.527, de 18 de novembro de 2011 (BRASIL, 2023).

Em 11 de julho de 2023, as respostas recebidas foram consolidadas e os resultados compilados estão apresentados na próxima seção.

RESULTADOS E DISCUSSÕES

Primeiramente, são apresentadas as respostas recebidas das UFs, organizadas em ordem alfabética, com destaques resumidos e sem qualquer identificação de respondentes. É importante ressaltar que a pesquisa realizada não tem o propósito de expor ou criticar qualquer participante, UF ou secretaria de segurança pública estadual que, por qualquer motivo, não tenha compreendido as questões, não tenha tido condições de enviar as respostas ou que não tenha recebido, por qualquer motivo, os e-mails e demais tentativas de contato por parte dos pesquisadores.

Respostas dos 26 estados e distrito federal

O estado do Acre (AC) solicitou abertura de processo SEI para recebimento das respostas, em 29 de maio de 2023, que detalham que o estado utiliza tecnologia de Inteligência Artificial em procedimentos por meio do Apolo, Cerco Eletrônico e Videomonitoramento, o que viabiliza a análise e interpretação de grandes volumes de dados (Big Data). As mencionadas tecnologias permitem a "identificação automática de padrões nos dados, o que reduz significativamente o tempo de análise e torna os resultados obtidos mais precisos e relevantes, ou seja, machine learning". O Apolo é um aplicativo desenvolvido pela Secretaria de Estado de Justiça e Segurança Pública do Acre (Sejusp) que auxilia na recuperação de veículos roubados por meio de tecnologia de reconhecimento facial. Em entrevista no início de janeiro, o chefe do Departamento de Modernização Tecnológica da Informação e Comunicação da Sejusp (DMITIC), Alexandre de Souza, explicou que a tecnologia é rápida em determinar a identidade das pessoas: "O sistema Apolo permite mais rapidez na identificação de pessoas suspeitas de crimes, por meio de um aplicativo de celular que já é operado pelos agentes de segurança pública em todo o estado" (VERUS, 2023).

A secretaria de Alagoas (AL) respondeu à pesquisa em 31 de janeiro de 2023 com a seguinte declaração "salientamos que as tecnologias usadas por essa Assessoria para produção de análise estão baseadas nas ferramentas de produção e gestão de bancos de dados, Business Intelligence (BI) e ferramentas de Geographic Information System (GIS)".

Em 19 de junho 2023, a Secretaria da Segurança Pública da Bahia (SSP/BA) mencionou a utilização de IA “nas soluções de reconhecimento facial e de identificação de placas veiculares nos alertas gerados por essas soluções e encaminhadas para a central de operações”. A resposta apresentada também destacou um sistema de videomonitoramento com Machine Learning “que permite que seu sistema aprenda e melhore automaticamente a partir dos dados capturados sem serem explicitamente programados”.

Do Distrito Federal (DF), em resposta recebida em 23 de maio 2023, o Subsecretário de Gestão da Informação mencionou a adoção de “métodos estatísticos para apuração de dados qualitativos e quantitativos, usando ferramentas de banco de dados e de Geoprocessamento para extração e modelagem dos dados”. Nessa UF, também são utilizadas técnicas de estatística inferencial para projeção dos dados e análise preditiva por equipe especializada, sem o uso de “tecnologia de inteligência artificial para modelagem de dados”.

A secretaria do Espírito Santo (ES), em resposta por e-mail enviada em 30 de maio de 2023, relatou que a “SESP está em processo de implantação de solução integrada de inteligência e processamento analítico”. Essa solução integra “software para análise preditiva, ciência de dados e aprendizado de máquina e software de ambiente hadoop para armazenagem e processamento de dados em ambiente big data, com projetos voltados para todas as forças de segurança do estado”. Também foi mencionado o serviço chamado “Cadastro Inteligente”, disponível a todos os interessados, que permite o cadastro preventivo do número de celular para eventuais ocorrências, e está integrado “aos sistemas dos órgãos de segurança pública (PC/PM), ampliando a possibilidade de devolução nos casos de furto, roubo ou perda, já que todas as informações necessárias para identificação do aparelho estarão previamente armazenadas”.

A resposta recebida pelo estado de Goiás (GO), em 28 de fevereiro de 2023, informou que o estado não adota Inteligência Artificial em seus procedimentos, e as “tecnologias como, big data, IoT e machine learning são utilizadas apenas para coleta de dados para posterior análise e formação de dados estatísticos e de políticas de segurança pública”.

Embora o estado do Maranhão (MA) tenha emitido o Parecer 295/2023 – ASSEJUR/SSP/MA, favorável ao envio das respostas, não foram fornecidas quaisquer respostas às questões da pesquisa.

O Mato Grosso (MT), em 17 de maio de 2023, emitiu o Despacho 35594/2023/SOV/SESP mencionando que a Secretaria Adjunta de Inteligência (SAI/SESP) não adota recursos de Inteligência Artificial implementados nos sistemas, mas expressou a intenção de adotá-lo em breve. Quanto às demais tecnologias, não são utilizadas.

Mato Grosso do Sul (MS), em 01 de fevereiro de 2023, respondeu ao e-mail mencionando que as forças Policiais de Mato Grosso do Sul utilizam “o sistema SIGO – Sistema Integrado de Gestão Operacional. Este sistema não possui nenhum recurso de inteligência aplicada aos dados, como reconhecimento facial ou algoritmos de *text mining* (mineração de textos)”.

A Secretaria de Estado de Justiça e Segurança Pública (Sejusp) de Minas Gerais (MG) respondeu à solicitação em 14 de fevereiro de 2023. Na resposta, mencionou que até aquela data não havia a utilização das tecnologias (Big Data, IoT e Machine

Learning) aplicadas a bancos de dados dos sistemas de segurança gerenciados pela SEJUSP, nem qualquer aplicação de inteligência artificial. Entretanto, a resposta indicou que estava em andamento a construção um *data lake*, para “implantação de tais tecnologias no futuro”.

Do Pará (PA), em 24 de janeiro de 2023, houve uma solicitação de cadastro no Serviço de Informação ao Cidadão, e a resposta foi postada no sistema minutos após esse procedimento. O conteúdo da resposta afirmou que a Diretoria de Estatística e Análise Criminal - DEAC/SIAC/SEGUP/PA utiliza uma aplicação denominada ORÁCULO, que realiza a leitura dos relatos das ocorrências policiais no intuito de classificar os delitos. Esta aplicação utiliza “Inteligência Artificial implementada com foco no Machine Learning”, e está centrada no conceito de descoberta de conhecimento em bases de dados (KDD), por meio de treinamento de Redes Neurais Artificiais com dados de ocorrências de anos anteriores ao atual. O objetivo dessa iniciativa é a identificação de “padrões textuais determinantes para a classificação da ocorrência em relação sua respectiva classe esperada, resultando em um modelo treinado”. O modelo treinado é inserido “na metodologia de análise das ocorrências diárias que chegam à esta Diretoria, através da classificação dos relatos em classes determinadas pelo aprendizado construído”.

Da Paraíba (PB), no dia 01 de fevereiro de 2023, por e-mail, a resposta foi “não utilizamos tecnologias de inteligência artificial para produção das nossas estatísticas” ou quaisquer das tecnologias mencionadas (Big Data, IoT e Machine Learning).

A resposta do estado Paraná (PR) foi enviada em 06 de junho de 2023 pela Coordenadoria das Delegacias da Mulher (CODEM), após registro da solicitação no formulário da Ouvidoria estadual. De acordo com as atribuições previstas pelo Decreto 7064/2013, essa unidade de segurança está restrita ao tema violência de gênero relacionada ao trabalho das Delegacias da Mulher do Estado (21 unidades). Na resposta, foi informado que a Polícia Civil do estado não utiliza tecnologias de IA para enfrentamento da violência de gênero, mas que está desenvolvendo um estudo, em parceria com o Banco Interamericano de Desenvolvimento e o CAPE/SESP, “para desenvolvimento de tecnologia apta a indicar os casos com maior risco de vulnerabilidade”. Uma das funcionalidades previstas para o sistema é a “indicação de alerta para os casos com maior risco à vida da vítima mulher, durante ou logo após o registro do boletim de ocorrência, gerando um indicativo de prioridade a ser dada ao caso”. Foi mencionado ainda que o mesmo algoritmo já é utilizado no estado do Ceará e terá como fonte de entrada o banco de dados do Boletim de Ocorrência Unificado (BOU) do estado do Paraná.

Como resposta, Pernambuco (PE) enviou, em 09 de maio de 2023, a Portaria Nº 752, nº 036, de 18 de fevereiro de 2023, que afirmava que “o acesso de qualquer interessado às informações de ocorrências policiais, dados criminais ou outras informações no âmbito da Secretaria de Defesa Social” (PERNAMBUCO, 2023). A referida Portaria menciona, no Art. 3º, a possibilidade de solicitação dos dados por meio de Pedido de Acesso à Informação – PAI no sítio eletrônico da Ouvidoria Geral do Estado. Tal registro foi realizado em 19 de junho de 2023, mas não houve retorno até a data de conclusão desta pesquisa.

Em 11 de maio de 2023, o Rio de Janeiro (RJ) solicitou vários documentos, incluindo cópia de documentos pessoais de todos os responsáveis pela pesquisa, e

houve deferimento da pesquisa. Contudo, até o fechamento deste levantamento, nenhuma resposta foi recebida.

O Rio Grande do Norte (RN) encaminhou, em 08 de julho de 2023, a solicitação para imprensa.sesed@gmail.com e não foi recebida resposta.

Em 02 de março de 2023, o Rio Grande do Sul (RS) respondeu que não utiliza qualquer uma das tecnologias elencadas.

Rondônia (RO), por meio da Secretaria de Estado da Segurança, Defesa e Cidadania (SESDEC), respondeu em 22 de maio de 2023 o seguinte: “Gerência de Tecnologia não se utiliza de máquinas que possuam Inteligência Artificial em seus procedimentos, nem dos demais recursos apontados, quais sejam Big data, IoT e Machine Learning”.

Em relação a Santa Catarina (SC), a resposta recebida em 07 de julho de 2023 foi “Não utilizamos nenhuma tecnologia de inteligência artificial”, ainda que no portal da Secretaria de Segurança Pública exista a veiculação realizada pelo governo do estado de “investimento em softwares para reconhecimento facial em câmeras capazes de ler letras e números automaticamente”, ou seja, uso de Inteligência Artificial. Inclusive, realizando-se busca no portal pelo termo “reconhecimento facial”, em 06 de julho de 2023, são retornados 10 resultados com câmeras em funcionamento desde 2018 (SANTA CATARINA, 2023).

A Secretaria de Segurança Pública de São Paulo (SP), em 12 de junho de 2023, respondeu que utiliza o software PowerBI “para analisar os dados transformando em business intelligence, fontes de dados em dashboards visuais”.

Do estado de Sergipe (SE), após novo contato, em 09 de maio de 2023, foi recebida a seguinte resposta: “Ao passo em que acusamos recebimento informamos que redirecionamos a demanda ao Núcleo de Apoio à Pesquisa em Segurança Pública e Cidadania (NAPSEC) - napsec@ssp.se.gov.br”. Desde então, nenhum retorno adicional foi recebido.

Ainda na mesma data, 09 de maio de 2023, do Tocantins (TO) foram recebidas pelo sistema Fala.BR, as respostas negativas para adoção de qualquer uma das quatro mencionadas tecnologias.

Em 01 de agosto de 2023, o estado de Roraima (RR) enviou resposta pelo Fala.br “foi verificado junto aos demais setores da Pasta e, atualmente, não há nenhum tipo de tecnologia de inteligência artificial em operação no âmbito da Secretaria de Estado de Segurança Pública de Roraima”.

Dos estados Amapá (AP), Amazonas (AM), Ceará (CE) e Piauí (PI) não foram recebidos retornos para estes dois questionamentos nas diversas (pelo menos duas) tentativas de contato incluindo as respectivas ouvidorias estaduais.

Pesquisa Processual

Gerar PDF

Autuação	
Processo:	00027_006398/2023-94
Tipo:	Documento Oficial: Ofício, Memorando, Portaria, Edital, Instrução Normativa e outros
Data de Registro:	08/08/2023
Interessados:	

Processo ou Documento de Acesso Restrito - Para condições de acesso verifique a [Condição de Acesso](#). Entre em contato com o órgão e/ou Unidade onde foi aberto ou onde se encontra o processo conforme andamento consultado. O respectivo contato pode ser encontrado no site institucional do referido órgão.

Lista de Protocolos (3 registros):

<input checked="" type="checkbox"/>	Documento / Processo	Tipo de Documento	Data do Documento	Data de Registro	Unidade
<input type="checkbox"/>	8708873	Anexo NUP 03377_2023_004086-37 - LAI	08/08/2023	08/08/2023	SSP-PIGAB/OLVIDORIA
<input type="checkbox"/>	8708892	Memorando 109	08/08/2023	08/08/2023	SSP-PIGAB/OLVIDORIA
<input type="checkbox"/>	8836966	SSP_Despacho GAB 2616	24/08/2023	24/08/2023	SSP-PIGAB

Lista de Andamentos (5 registros):

Data/Hora	Unidade	Descrição
25/06/2023 15:08	SSP-PI/SO/DINTE	Processo recebido na unidade
24/08/2023 15:36	SSP-PI/SO/DINTE	Processo remetido pela unidade SSP-PIGAB
10/08/2023 10:19	SSP-PIGAB	Processo recebido na unidade
08/08/2023 10:55	SSP-PIGAB	Processo remetido pela unidade SSP-PIGAB/OLVIDORIA
08/08/2023 10:50	SSP-PIGAB/OLVIDORIA	Processo público gerado

Análises dos resultados

O estado do TO requereu o cadastro da solicitação no sistema Fala.BR para o envio das respostas. Em 19 de junho 2023, outros quatro estados (MS, SC, PI e RR) ainda não haviam respondido aos e-mails e, por esse motivo, também foram cadastrados no mesmo sistema. MS e SC responderam dentro do prazo solicitado (01/07/2023), enquanto RR respondeu em 01/08/2023 e PI encaminhou a solicitação para um processo SEI que foi respondido, em 24/08/2023, por meio de um despacho restrito ao qual os pesquisadores não tiveram acesso.

Das respostas recebidas, duas mencionam o uso de sistema de visualização – Business Intelligence (BI) (AL e SP) e duas citaram sistemas de geoprocessamento (GIS) (AL e DF). Entre as 27 UFs, quatro estão em processo de adoção ou considerando a adoção de alguma das citadas tecnologias (ES, MT, MG e PR).

Apenas o estado do Pará mencionou o uso de Redes Neurais Artificiais para *text mining*, enquanto o estado de Minas Gerais foi o único a citar a criação de um *data lake*. Os demais estados não mencionaram métodos ou tecnologias específicas.

No detalhamento das utilizações, o Acre e a Bahia mencionaram o reconhecimento facial, enquanto a Bahia também mencionou o reconhecimento de placas, conforme Figura 1.

Figura 1 – Resumo das respostas das 27 Unidades da Federação do Brasil

UF	Resposta*	Dias	IA	ML	IOT	BD	NU	SR	Observações
Acre	29/05	126	●	●	●	●			Processo SEI, Reconhecimento facial
Alagoas	31/01	8					●		BI, GIS
Amapá								○	
Amazonas	10/04	77						○	
Bahia	19/06	147	●	●	●				Reconhecimento facial, reconhecimento de placas
Ceará								○	
Distrito Federal	23/05	120					●		Estatística, GIS
Espírito Santo	30/05	127	●	●					Processo de implantação
Goiás	28/02	36		●	●	●			
Maranhão								●	Parecer 295/2023 - ASSEJUR/SSP/MA favorável ao envio das respostas Previsão de adoção
Mato Grosso	17/05	114	●						
Mato Grosso do Sul	01/02	9					●		
Minas Gerais	14/02	22					●		Previsão de adoção e criação de data lake
Pará	24/01	1	●	●					Serviço de Informação ao Cidadão, RNA, text mining
Paraíba	01/02	9					●		
Paraná	06/06	134					●		Ouvidoria estadual, Previsão de adoção
Pernambuco	09/05	106						●	Ouvidoria Geral do Estado - sem resposta
Piauí	01/09	221						●	Encaminhado e respondido por despacho restrito
Rio de Janeiro	11/05	108						●	Pesquisa deferida
Rio Grande do Norte	08/07	166						●	Encaminhado para imprensa.sesed@gmail.com
Rio Grande do Sul	02/03	38					●		
Rondônia	22/05	119					●		
Roraima	01/08	190					●		
Santa Catarina	07/07	165					●		
São Paulo	12/06	140					●		BI
Sergipe	09/05	106						●	Encaminhado para napsec@ssp.se.gov.br
Tocantins	09/05	106					●		
TOTAIS		100	5	5	3	2	12	9	

*Todas as respostas foram enviadas durante o ano de 2023.

Legenda: IA: Inteligência Artificial ML: Machine Learning IOT: Internet das Coisas BD: Banco de Dados NU: Não Utilização SR: Sem Resposta

Fonte: Os autores (2024)

Quanto ao uso das tecnologias Inteligência Artificial (IA), cinco estados (18,52%) mencionaram que usam: AC, BA, ES, MT e PA. Em relação ao Machine Learning (ML), cinco (18,52%) mencionaram seu uso: AC, BA, ES, GO e PA. Isso significa que seis estados utilizam algum tipo de inteligência artificial (22,22%). Quanto ao uso de Internet das Coisas (IoT), três estados mencionaram seu uso: AC, BA e GO e Big Data (BD), dois estados (7,41%): AC e GO.

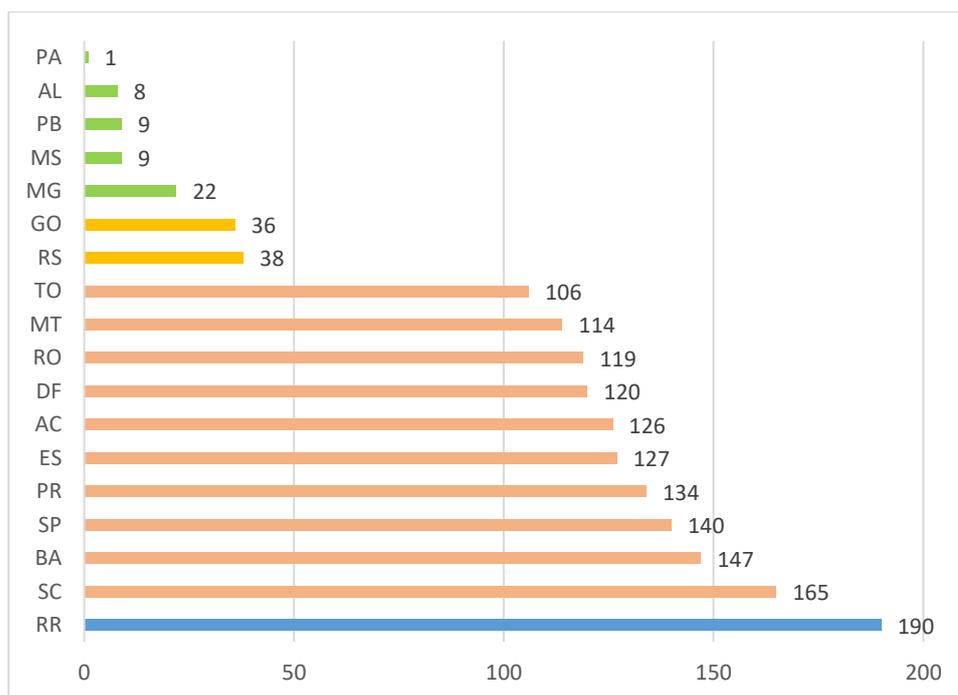
Para os estados que não utilizam nenhuma das tecnologias mencionadas, foi utilizada a coluna “NU” (Não Utilização). Neste grupo, estão enquadradas as respostas de 11 estados (AL, MS, MG, PB, PR, RS, RO, RR, SC, SP e TO), além do Distrito Federal. No entanto, de forma contraditória às respostas enviadas, o estado de Alagoas (ALAGOAS, 2023) divulgou em 27 de junho de 2023 uma nova sala no Centro Integrado da Segurança Pública que passa a utilizar “Inteligência Artificial para avançar na redução da violência no Estado”. Da mesma forma, o Paraná veiculou por meio da Agência Estadual de Notícias, em 29 de junho 2022, o desenvolvimento dos projetos “Falcão” e “Olho Vivo, Paraná” para ampliar e modernizar os sistemas de segurança pública com a promessa de “transformar a fiscalização, monitoramento e repressão no Paraná, fazendo da Inteligência Artificial (IA) uma das principais aliadas contra o crime organizado” (PARANÁ, 2022).

Os estados que não responderam à pesquisa estão indicados na coluna “SR” (Sem Resposta). Nesta categoria, estão três estados (círculos sem preenchimento) que não enviaram qualquer tipo de retorno (AP, AM e CE), além de outros seis estados (MA, PE, PI, RJ, RN e SE) que acusaram recebimento, encaminharam a

demanda, mas não responderam às questões da pesquisa ou não forneceram acesso ao despacho com o teor da resposta. É pertinente observar que o estado do Amazonas não respondeu às duas questões propostas, mas enviou os microdados de feminicídio e violência doméstica para análises, que são objetos de outra pesquisa em desenvolvimento. Em resumo, 9 estados não enviaram as respostas, representando 33,33% do total.

Na medição de tempo de resposta foi considerada a quantidade de dias decorridos desde a data do envio do primeiro e-mail (23 de janeiro de 2023) e a data do recebimento da resposta às duas questões propostas. Em cumprimento ao artigo 11º, §1º da Lei nº 12.527, de 18 de novembro de 2011 (BRASIL, 2011), o acesso às informações requisitadas deve ser imediato e, em não o sendo possível, a resposta deve ocorrer no prazo máximo de 20 (vinte) dias (prorrogáveis por mais 10 dias – mediante justificativa expressa), contados a partir da solicitação. Desta forma, no Gráfico 1 foi adotado o seguinte critério: respostas até 30 dias (inclusive) – dentro do prazo legal – em verde, respostas até 60 dias (inclusive) – acima do prazo legal em 30 dias – em amarelo, entre 61 e 180 dias – em salmão e acima de 180 dias em azul. As 9 UFs que não enviaram respostas não estão representadas no Gráfico 1.

Gráfico 1 – Tempo, em dias, do prazo de resposta dos 18 estados



Fonte: Os autores (2024)

Em média foram 96 dias para recebimento das respostas das 18 UFs. Apenas os estados do PA, AL, PB, MS e MG responderam em menos de 30 dias e 11 estados demoraram mais de três meses para o envio das respostas.

CONSIDERAÇÕES FINAIS

Ao adotar o uso de tecnologias disruptivas, qualquer área enfrentará benefícios e desafios específicos. Na segurança pública não é diferente,

especialmente considerando os desafios enfrentados pelo Brasil nesse campo, com altos índices de criminalidade em diferentes formas de violências e em várias regiões do país. No entanto, é justamente nesses contextos sociais adversos que o uso de tecnologias pode desempenhar um papel essencial na prevenção e combate ao crime, contribuindo para aprimorar a eficiência das operações de segurança pública.

Esta pesquisa demonstra que no Brasil já estão em curso iniciativas que exploram o uso das mencionadas tecnologias disruptivas na segurança pública. As aplicações se concentram em tarefas como reconhecimento facial, reconhecimento de placas veiculares e mineração de textos, entre outras. Além disso, observa-se que alguns estados que ainda não adotam efetivamente essas tecnologias estão empenhados em fazê-lo a curto prazo. No entanto, é essencial ressaltar que a implementação de tecnologias disruptivas, em especial aquelas que utilizam dados biométricos, não possui uma legislação adequada no país. Portanto, para minimizar erros relacionados a particularidades demográficas, é fundamental que esse avanço tecnológico em questão seja aderente ao contexto cultural brasileiro, reduzindo eventuais vieses nos algoritmos (Oliveira et al., 2022).

Além de questões éticas e legais relacionadas à preservação de dados pessoais, resultados indicam que o Brasil enfrenta desafios significativos no uso dessas tecnologias. Há obstáculos relacionados à infraestrutura tecnológica e à capacidade de implementação e implantação dessas tecnologias na segurança pública em todo o país. Restrições de recursos financeiros e a falta de conhecimento especializado são alguns dos principais fatores que contribuem para essas adversidades. No entanto, merece destaque a constatação da falta de integração entre as entidades responsáveis pela segurança pública nas UFs, ou ainda uma unidade que tenha uma visão holística da área. Fato confirmado pela resposta recebida, por exemplo do estado de SC, que menciona a não utilização das tecnologias quando essas estão em efetivo uso para reconhecimento facial e leitura automática de placas de carro com auxílio de câmeras em áreas públicas.

Adicionalmente, as dificuldades encontradas pelos pesquisadores na coleta de informações junto às instituições de segurança pública, que resultaram em respostas incompletas, inconsistentes ou não enviadas, podem ser atribuídas ainda a diversos outros fatores. Entre eles, destacam-se a escassez de pessoal, falta de recursos financeiros, excesso de burocracia, falta de padronização nos processos e ausência de uma cultura de transparência nessas instituições.

É de conhecimento comum que a ciência pode desempenhar papel crítico na segurança pública, fornecendo conhecimentos, ferramentas e abordagens necessárias para lidar com desafios complexos e garantir a proteção da sociedade de maneira eficaz e ética. O contínuo avanço científico é essencial para melhorar continuamente as estratégias de segurança e promover um ambiente mais seguro para todos. A promoção de parcerias entre as instituições de ensino e instituições de segurança pública, com a devida consideração a termos de sigilo, responsabilidade e outros mecanismos legais, pode auxiliar a superar algumas dessas dificuldades.

Além disso, é fundamental estabelecer bases de dados unificadas, padronizar os processos de coleta e registro de informações em todas as unidades federativas, e disponibilizar regularmente dados atualizados para pesquisas e análises. Enquanto houver uma barreira entre a academia e as instituições de segurança

pública, haverá atraso na produção e aplicação de conhecimentos científicos desenvolvidos para mitigar os problemas de segurança pública no Brasil, o que traz graves prejuízos – principalmente – para a sociedade.

Disruptive technologies in public safety: a Brazilian situational analysis

ABSTRACT

This article investigates the use of disruptive technologies, such as Artificial Intelligence, Big Data, Machine Learning and Internet of Things, as tools to support public security activities in the 27 Federation Units (UFs) in Brazil. In addition, the study evaluates the dissemination of data and information by state public security institutions to researchers, as well as the response time. Through contacts (emails, systems, websites, ombudsman and others) with the 27 FUs, it was possible to obtain information on the adoption of these technologies and point out challenges faced. The results reveal that six states (22.22%) adopt - at least one - of the technologies surveyed, while four (14.81%) mentioned adoption initiatives. On the other hand, 12 states (44.44%) said they do not use the technologies mentioned and another 9 (33.33%) did not respond to the contacts made. The survey highlights the importance of partnerships between educational institutions and public security institutions, as well as national standardization and sharing of updated data for research and analysis.

KEYWORDS: Artificial intelligence. Big data. Internet of things. Machine learning. Disruptive.

AGRADECIMENTOS

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES), Edital nº 16/2020 - PROCAD Segurança Pública e Ciências Forenses, Projeto Curadoria Digital de Dados e Informações para prevenção da violência nas famílias e comunidades.

REFERÊNCIAS

ALAGOAS. Secretaria de Segurança Pública. **Centro Integrado da Segurança Pública usa inteligência artificial para avançar na redução da violência no Estado**. 27/06/2023. Disponível em: <http://seguranca.al.gov.br/noticia/2023/06/27/centro-integrado-da-seguranca-publica-usa-inteligencia-artificial-para-avancar-na-reducao-da-violencia-no-estado/>. Acesso em: 11 jul. 2023.

BRASIL. Controladoria-Geral da União (CGU). **Novos enunciados CGU**. 2023. Disponível em: <https://www.gov.br/acessoinformacao/pt-br/lai-para-sic/transparencia-passiva/guias-e-orientacoes/enunciados-da-lai/@@download/file/NOVOS%20ENUNCIADOS%20LAI%20CGU%203-fev-2023.pdf>. Acesso em: 10 abr. 2024.

BRASIL. **Lei no 12.527, de 18 de novembro de 2011**, Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal [...]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 17 jul. 2023.

CHRISTENSEN, C. M. . **O dilema da inovação**: quando as novas tecnologias levam empresas ao fracasso. São Paulo: M. Books do Brasil Editora. 2012.

FERREIRA, H. R. S.; MARCIAL, E. C. . **Violência e segurança pública em 2023**: cenários exploratórios e planejamento prospectivo. 2015. Disponível em: <https://repositorio.ipea.gov.br/handle/11058/5680>. Acesso em: 11 jul. 2023.

INSTITUTE FOR ECONOMICS & PIECE (IEP). **Global Peace Index 2023**: measuring peace in a complex world, Sydney, June 2023. Disponível em: <https://www.visionofhumanity.org/wp-content/uploads/2023/06/GPI-2023-Web.pdf>. Acesso em: 10 jul. 2023.

OLIVEIRA, L. V.; CRIPPA, M. E. N.; LAURENTE GRADOS, Í. J.; HOLANDA, T. D. L. C. Aspectos ético-jurídicos e tecnológicos do emprego de reconhecimento facial na segurança pública no Brasil. **Revista Tecnologia e Sociedade**, v. 18, n. 50, p. 114, 2 jan. 2022. Disponível em: <https://periodicos.utfpr.edu.br/rts/article/view/12968>. Acesso em: 10 jul. 2023.

PARANÁ. Agência estadual de notícias. **Com os projetos Falcão e Olho Vivo, Paraná amplia e moderniza sistemas de segurança pública.** 29/06/2022. Disponível em: <https://www.aen.pr.gov.br/Noticia/Com-os-projetos-Falcao-e-Olho-Vivo-Parana-amplia-e-moderniza-sistemas-de-seguranca-publica>. Acesso em: 11 jul. 2023.

PERNAMBUCO. **Portaria Nº 752**, nº 036, de 18/02/2023. Disponível em: https://www.sds.pe.gov.br/images/media/1676731470_036%20BGSDS%20DE%2018FEV2023.pdf. Acesso em: 21 jun. 2023.

SANTA CATARINA. **Secretaria de Segurança Pública.** 16/07/2021. Disponível em: <https://www.ssp.sc.gov.br/index.php/component/content/article/87-noticias/2313-governo-reforca-sistemas-de-inteligencia-e-tecnologia-para-ampliar-seguranca?Itemid=437>. Acesso em: 06 jul. 2023.

SILVA, B. L.; LIMEIRA, M. L. C. . As novas tecnologias e a segurança pública: um casamento complexo e promissor. 2023. In: **Pro Lege Vigilanda**. Disponível em: <https://periodicos.esbm.org.br/index.php/prolegevigilanda/article/view/26>. Acesso em: 10 abr. 2024.

VERUS, I. . Aplicativo da Sejusp ajuda Polícia Militar do Amazonas a recuperar veículos roubados. In.: **Jornal Notícias do Acre.** 2023. Disponível em: <https://agencia.ac.gov.br/aplicativo-da-sejusp-ajuda-policia-militar-do-amazonas-a-recuperar-veiculos-roubados/>. Acesso em: 09 jul. 2023.

VIEIRA, L. M. . A problemática da inteligência artificial e dos vieses algorítmicos: caso Compas. **Anais** do 2019 Brazilian Technology Symposium. Disponível em: <https://lcv.fee.unicamp.br/images/BTSym-19/Papers/090.pdf>. Acesso em: 09 abr. 2024.

TSUNODA, D. F.; CANDIDO, A. C. . Tecnologia disruptiva e segurança pública: uma análise da produção científica mundial. **Research, Society and Development**, v. 11, p. 1-24, 2022. Disponível em: <https://rsdjournal.org/index.php/rsd/article/view/38647>. Acesso em: 10 jul. 2023.

Recebido: 12/04/2024

Aprovado: 11/07/2024

DOI: 10.3895/rts.v20n61.18408

Como citar:

TSUNODA, Denise Fukumi; CÂNDIDO, Ana Clara; GUIMARÃES, André José Ribeiro. Tecnologias disruptivas em segurança pública: uma análise situacional brasileira. **Tecnol. Soc.**, Curitiba, v. 20, n. 61, p. 317-333, jul./set., 2024. Disponível em:

<https://periodicos.utfrpr.edu.br/rts/article/view/18408>

Acesso em: XXX.

Correspondência:

Direito autoral: Este artigo está licenciado sob os termos da Licença Creative Commons-Atribuição 4.0 Internacional.

