

# Inteligência artificial no combate à fraude e corrupção: A experiência da Controladoria Geral do Município do Rio de Janeiro<sup>1</sup>

*Combating fraud and corruption with artificial intelligence: Rio de Janeiro Municipality Comptroller's Office experience*

*Inteligencia artificial en combate al fraude y corrupción: La experiencia de la Contraloría General del Municipio de Río de Janeiro*

*Dalton Henrique Mota Ibere Gilson e Gustavo de Avellar Bramili*

<https://doi.org/10.36428/revistadacgu.v14i27.531>

**Resumo:** O combate aos atos de corrupção e improbidade na administração pública brasileira é uma questão de grande importância e complexidade. Este artigo descreve o projeto de Inteligência Artificial que está sendo desenvolvido pela Controladoria Geral do Município do Rio de Janeiro para contribuir no combate à corrupção. Este projeto utiliza dados de contratos municipais e da execução orçamentária em conjunto com fatores de risco definidos a priori para estimar algoritmos de *Machine Learning*, com o objetivo de detectar sinais indicando alto risco de corrupção nas secretarias municipais e nas empresas da administração indireta. No artigo são apresentadas as etapas do projeto que está sendo implementado, os desafios e as limitações encontradas até o seu atual estágio de desenvolvimento. A partir dos resultados preliminares das tipologias já estimadas, avaliamos que as expectativas sobre o desempenho da ferramenta são promissoras.

**Palavras-chave:** Inteligência Artificial. *Machine Learning*. Controladoria Geral do Município do Rio de Janeiro. Detecção de Fraude. Combate à Corrupção.

**Abstract:** The fight against corruption and malfeasance in the Brazilian public administration is a matter of great importance and complexity. This article describes the Artificial Intelligence project being developed by the Municipal Comptroller's Office of Rio de Janeiro to contribute to the fight against corruption. This project uses data from municipal contracts and budget execution, combined with pre-defined risk factors, to estimate Machine Learning algorithms aimed at detecting signs indicating a high risk of corruption in municipal secretariats and indirect public administration companies. The article presents the stages of the project being implemented, the challenges and limitations encountered up to its current development stage. Based on preliminary results from estimated parameters, we evaluate that expectations regarding the tool's performance are promising.

1. Artigo submetido em 14/07/2022 e aceito em 03/04/2023

**Keywords :** Artificial Intelligence. Machine Learning. Rio de Janeiro Municipality Comptroller's Office. Fraud Detection. Fighting Corruption.

**Resumen:** La lucha contra los actos de corrupción e improbidad en la administración pública brasileña es una cuestión de gran importancia y complejidad. Este artículo describe el proyecto de Inteligencia Artificial que está siendo desarrollado por la Contraloría General del Municipio de Río de Janeiro para contribuir en la lucha contra la corrupción. Este proyecto utiliza datos de contratos municipales y de la ejecución presupuestaria en conjunto con factores de riesgo definidos a priori para estimar algoritmos de *Machine Learning*, con el objetivo de detectar señales indicando alto riesgo de corrupción en las secretarías municipales y en las empresas de la administración indirecta. En el artículo se presentan las etapas del proyecto que está siendo implementado, los desafíos y las limitaciones encontradas hasta su actual etapa de desarrollo. A partir de los resultados preliminares de las tipologías ya estimadas, evaluamos que las expectativas sobre el rendimiento de la herramienta son prometedoras.

**Palabras clave :** Inteligencia Artificial. *Machine Learning*. Contraloría. Detección de fraude. Lucha contra la corrupción.

## INTRODUÇÃO

A Controladoria Geral do Município do Rio de Janeiro (CGM-RJ) foi o primeiro órgão de controladoria criado no Brasil, no ano de 1993, pela Lei Municipal no 2068, de 22 de Dezembro de 1993. Ao longo desses quase trinta anos, muitos desafios se fizeram presentes, dentre eles o de estar sempre atualizado com as melhores práticas de gestão e equipado com as melhores ferramentas tecnológicas disponíveis para executar sua missão institucional.

Com efeito, a criação do sistema FINCON – Sistema de Contabilidade e Execução Orçamentária - pelo Município do Rio de Janeiro, ainda na década de 80, permitiu o registro dos fatos relacionados aos processos administrativos de despesas e execução orçamentária, e a realização da contabilização dos eventos orçamentários, financeiros e patrimoniais, com base nas legislações de licitações e orçamentárias. Associado ao sistema FINCON está o sistema de Controle de Contratos – FCTR, implementado na década de 90, que realiza o controle do cadastro e da execução orçamentária dos instrumentos contratuais de despesa e dos convênios de receita.

Com os registros das informações feitas pelos sistemas FINCON e FCTR ao longo dos anos, foram gerados e estão armazenados hoje na Controladoria Geral do Município do RJ mais de 10 Terabytes<sup>2</sup> de dados destes sistemas. Uma primeira ação no sentido de utilizar esses dados através de uma interface gerencial, visando dar suporte ao trabalho dos téc-

nicos da controladoria, se deu com a criação do SIG – Sistema de Informações Gerenciais, pela CGM-RJ, ainda na década de 90. A partir da regulamentação no âmbito municipal da Lei Federal 12.846/2013 – Lei anticorrupção, através do decreto municipal 46.195/2019, iniciaram-se as atividades de correição de pessoas jurídicas dentro do município do Rio de Janeiro, que pela primeira vez passou a ter o diploma legal para responsabilizar administrativamente as pessoas jurídicas por atos de corrupção.

Embora extremamente úteis às atividades até então realizadas pela CGM-RJ, os sistemas informatizados existentes se mostraram insuficientes para as necessidades da correição, em especial para a área de detecção e apuração de atos ímprobos, cujas atribuições incluem a identificação de transações e atos suspeitos de corrupção no Município do Rio de Janeiro – que tem um orçamento anual próximo aos R\$ 39 bilhões<sup>3</sup>, o segundo maior do país entre todos os municípios. Diante dessa necessidade, foram iniciadas internamente na Controladoria pesquisas com a finalidade de se verificar a viabilidade de desenvolver internamente uma solução analítica que pudesse solucionar o problema da corregedoria, que é o de expandir sua capacidade analítica de dados e otimizar a alocação dos recursos humanos disponíveis na tarefa de detecção e no enfrentamento de atos de improbidade.

2. Um Terabyte equivale a 1.024 gigabytes

3. Orçamento do Poder Executivo do Município do RJ de acordo com a LOA 2022.

As pesquisas internas convergiram para o atual projeto de Inteligência Artificial, que é sustentado por dois pilares básicos:

1. Busca de excelência técnica e aperfeiçoamento contínuo
2. Aderência a um estrito código de ética na condução de todo o processo.

Esses são os dois princípios que norteiam todo projeto de desenvolvimento de ferramentas de Inteligência Artificial no combate a corrupção no município do Rio de Janeiro, em fase intermediária de desenvolvimento, e que será descrito no presente artigo.

Para contextualizarmos o projeto da CGM a nível nacional, é importante destacarmos que a tecnologia de Inteligência Artificial já vem sendo utilizada com sucesso por diversos órgãos de controle do Brasil, como o Tribunal de Contas da União, a Controladoria Geral da União, Receita Federal, além de outros Tribunais de Contas e órgãos de controle estaduais, com objetivo de acelerar processos e garantir maior produtividade, efetividade e eficiência às atividades de controle. Podemos citar algumas dentre inúmeras iniciativas notáveis e premiadas, como sistema ALICE, que analisa preventivamente as licitações, além dos demais sistemas do TCU e da CGU, ADELE, MONICA e SOFIA, e também o Observatório da Despesa Pública, todos eles referências na utilização de tecnologia na área de controle em nosso país.

Este artigo prossegue com uma revisão da literatura internacional a respeito da utilização da IA no setor público, discutindo em seguida algumas evidências e a importância da questão ética nos projetos de IA. Depois discutiremos sobre aspectos técnicos essenciais da IA, e apresentaremos as etapas do projeto que está em desenvolvimento na CGM-RJ, falando sobre a escolha da tecnologia, sobre as cinco tipologias planejadas, e sobre o algoritmo de detecção de corrupção, concluindo com uma seção relatando os desafios, as limitações e os resultados preliminares obtidos até esta fase do projeto, registrando que esses resultados tem se revelado promissores.

## **INTELIGÊNCIA ARTIFICIAL NO SETOR PÚBLICO: REVISÃO DA LITERATURA**

O Avanço da Inteligência Artificial (IA) tem sido objeto de intensa pesquisa e prática tanto na academia quanto nos setores público e privado. Existe portanto, uma necessidade crescente de se compreender de forma integrada as aplicações da IA e os desafios associados a esse campo. Wirtz, Weyerer & Geyer (2018) realizaram uma revisão sistemática da literatura sobre aplicações de IA no setor público e concluíram que a maioria das pesquisas acadêmicas sobre o assunto não aborda de forma integrada aplicações e desafios, concentrando-se apenas em sub-áreas temáticas.

Estes autores propõem a categorização das pesquisas em cinco categorias principais: Serviços governamentais (categoria 1), impacto social e profissional da IA (categoria 2), lei e ordem pública relacionadas a IA (categoria 3), ética da IA (categoria 4) e políticas públicas de IA (categoria 5).

Os artigos da categoria 1 cobrem principalmente aplicações de IA com foco na melhoria dos fluxos de trabalho, modelos de previsão utilizando IA, gerenciamento de dados, bem como administração do conhecimento e tomada de decisões (Chou, Lin Pham & Shao, 2015; Chun & Wai, 2007; 2008; Kouziokas, 2017; Kouziokas, Chatzigeorgiou & Perakis, 2017, Sun & Medaglia, 2017; Zheng et al., 2018). Os artigos da categoria 2, por sua vez, contém estudos que enfatizam a IA e seu impacto no ambiente de trabalho e social. Em economias mais avançadas esse impacto pode estar associado a possibilidade de aumento do desemprego devido à substituição do trabalho humano por máquinas, enquanto que em economias em desenvolvimento as ferramentas de IA ainda estão bastante subutilizadas (Aguilera & Ramos Barrera, 2016, Bartlett, 2017; Chen, 2009). Os artigos da categoria 3 tratam de aspectos relacionados à ordem pública e as leis em vigor. Sob esses aspectos, a IA pode ser valiosa no gerenciamento de risco e apoio à previsão de desastres naturais como terremotos e enchentes, também podendo ser utilizada na vigilância, segurança pública e prevenção criminal (Tang & Wen, 2009; Power, 2016; Kouziokas, 2017; Quraishi, 2017). Já os artigos da categoria 4 tratam da ética associada às aplicações de IA com seus respectivos riscos e benefícios (Muller, 2014; Johnson, 2015; Massaro, Norton &

Kaminski, 2017, Quraishi, 2017) e, finalmente, os artigos da categoria 5 possuem foco nas políticas governamentais relacionadas à IA (Boyd & Wilson, 2017; Scherer, 2016; Thierer, O'Sullivan Castillo & Russell, 2017).

Ainda dentro do escopo da mesma revisão da literatura feita no artigo de Wirtz, Weyerer & Geyer (2018), esses autores identificam 17 estudos que analisam os desafios da IA no contexto do setor público. Essa análise indica que a IA vem provocando debates nos meios científicos e na sociedade a respeito dos impactos éticos e sociais, e também sobre a implementação dessas tecnologias no serviço público, bem como sobre as condições legais que regem sua atuação, incluindo regulamentos de privacidade e responsabilidade. Com base nessas linhas de debate, os autores propuseram quatro dimensões de desafios de IA no setor público: “Implementação de tecnologia de IA”, “Leis e Regulação de IA”, “Ética de IA” e “IA na Sociedade”.

O primeiro desafio “Implementação de tecnologia de IA” trata de diversas questões, tais como a segurança no uso das ferramentas de IA – no qual se deve estar atento e evitar a manipulação dessa tecnologia por humanos que tentem empregá-las com finalidades nocivas, também a questão da qualidade da integração entre sistemas e dados, uma vez que dados de qualidade são fundamentais para a correta performance da tecnologia IA, a questão da viabilidade financeira, pois é necessário que um projeto de IA seja bem planejado e suportado com orçamento que supra todas as necessidades de equipamentos, sistemas e pessoas envolvidas (o que nem sempre é possível), e finalmente a questão da especialização e do expertise, pois profissionais com conhecimento para atuar em projetos de IA no setor público são escassos.

O desafio relacionado a “Leis e Regulação de IA” se refere à governança geral de inteligência artificial, portanto à capacidade de administrar e controlar a tecnologia de IA e seus impactos sociais e econômicos. Essa governança está associada a múltiplos assuntos legais e regulatórios, pertinentes a dados, algoritmos, infraestruturas e seres humanos (Gasser, 2017). Dentre os desafios relacionados, estão a correta compreensão da atuação dos sistemas de inteligência autônomos chamados de *black-boxes*, além dos aspectos de responsabilização legal dos responsáveis pelas ferramentas de IA, e

finalmente o desafio de preservar dados pessoais e as ameaças à privacidade no contexto da utilização de IA.

Os assuntos relacionados à terceira dimensão de desafios, “Ética de IA”, são intensamente debatidos em conjunto com as aplicações de IA no setor público. A revisão de literatura revela que o desafio de ética da IA cobre um conjunto amplo de aspectos, desde a utilização de IA para criar regras de comportamento humano, compatibilidade dos valores humanos com a atuação e decisões de máquinas, dilemas morais e discriminações sociais no uso de IA. (Anderson & Anderson, 2011; Velasquez, Andre, Shanks & Meyer, 2010; Krausová, 2017)

O quinto desafio está relacionado a “IA na Sociedade” e trata da transição da vida social e das interações humanas como consequência da IA. (Cath et al., 2018; Johnson & Verdicchio, 2017)

Outra revisão da literatura, com foco maior no uso de IA especificamente contra corrupção, foi conduzida por Isabelle Adam e Mihály Fazekas (Adam & Fazekas, 2021), no qual buscaram identificar, através da revisão sistemática de resultados de diversos estudos publicados por pesquisadores de inúmeros países, se existem evidências suficientes para rejeitar ou não a hipótese de que a utilização de tecnologias de informação modernas no setor público, dentre elas (mas não apenas) a IA, tem efeito estritamente positivo do ponto de vista da obtenção de maior transparência, maior “accountability” e redução significativa da corrupção.

Para isso, buscaram responder as seguintes questões formuladas: Quais as principais aplicações tecnológicas contra a corrupção? Quais os impactos das ferramentas tecnológicas, tanto positivas quanto negativas? Quais são os fatores facilitadores e limitadores das ferramentas anti-corrupção baseadas em tecnologia?

Com relação a utilização de ferramentas tecnológicas e seu impacto individualizado no combate a corrupção no setor público, o estudo analisou as evidências de seis tipos de ferramentas, que citamos a seguir: 1) serviços públicos digitais, 2) plataformas de *crowdsourcing* 3) ferramentas de *whistleblowing* 4) portais de transparência 5) Blockchain/tecnologia de registros distribuídos e 6) Inteligência Artificial.

A respeito das evidências do uso de ferramentas de Inteligência Artificial no combate a corrupção no setor público, foco do presente projeto da Controla-

doria do Município do Rio de Janeiro, o estudo conclui que a IA tem sido útil no combate à corrupção devido a capacidade de revelar rapidamente padrões ocultos nos dados, possibilitando assim a identificação de situações suspeitas e o direcionamento dos esforços e dos recursos escassos das organizações públicas aos objetivos apropriados.

Os autores Nils Kobis, Christopher Starke e Iyad Rahwan (Kobis, Starke & Rahwan, 2022) analisam as promessas e perigos da utilização da IA no combate a corrupção, a partir da expectativa de que a utilização dessas tecnologias no setor público possa trazer uma mudança há muito tempo esperada nesse tema. Sob essa perspectiva, o estudo desses autores busca resumir as principais razões para a esperança depositada nessa ferramenta tecnológica, além de destacar os desafios a serem enfrentados, chamando atenção para os efeitos divergentes das tecnologias de IA nas estruturas de poder existentes.

Na análise desses autores, a Inteligência Artificial possui três importantes vantagens sobre os esforços tradicionais anti-corrupção. Primeiro, os sistemas de IA tais como *Machine Learning* podem ser dotados de habilidades de aprendizado automático. Muitos pesquisadores esperam que estas características sejam capazes de detectar e prever a corrupção. Em alguns projetos inovadores, a utilização de IA já pode automaticamente detectar zonas de risco para corrupção, utilizando um grande conjunto de reportagens de mídia, arquivos policiais e dados de autoridades financeiras para a previsão de diversos tipos de atos de improbidade.

Segundo, devido ao crescente poder computacional, a IA pode analisar conjuntos de dados de tamanho sem precedentes. Impulsionada por esta massa de dados disponíveis cada vez maior, os sistemas de IA tem obtido sucesso em detectar e classificar a atividade de corrupção. Por exemplo, a Microsoft recentemente anunciou seu projeto de solução de tecnologia de inteligência artificial<sup>4</sup>, oferecendo produtos anticorrupção para governos. Da mesma forma, as ferramentas de IA podem também investigar grandes “data leaks” tais como os *Pandoras Papers*<sup>5</sup> para revelar os padrões de corrupção – uma tarefa inviável para humanos.

Terceiro, a IA é imparcial. Os tomadores de decisão no serviço público muitas vezes enfrentam conflitos de interesse, o que é minimizado ou mesmo eliminado quando se retira o ser humano do processo.

Já com relação aos desafios, o primeiro desafio identificado no trabalho desses autores é o desafio dos dados. A obtenção de dados confiáveis e válidos para serem utilizados representa um desafio particularmente espinhoso no combate a corrupção. Além disso, não é simples definir quais indicadores servem de *proxies* válidas para a corrupção, e como se mensurar este fenômeno, que é por definição oculto.

O segundo é o desafio de interpretar com devido cuidado os resultados dos algoritmos, uma vez que não são raras as ocorrências de falsos positivos, e assim sendo existe o risco de se classificar erroneamente indivíduos inocentes como “corruptos”.

O terceiro é o desafio humano, que se refere ao contexto socioeconômico no qual os algoritmos operam e ao dilema ético de se deixar os algoritmos terem eventualmente a palavra final.

## EVIDÊNCIAS DA UTILIZAÇÃO DE IA NO SETOR PÚBLICO

Adam & Fazekas (2021) dividem, para fins analíticos, a corrupção entre a pequena corrupção e a grande corrupção. A pequena corrupção em grande medida se refere a burocratas se utilizando do cargo público e de sua influência para ganhos ilegais, tais como subornos, fraudes, etc. Neste caso, a pequena corrupção pode ser compreendida dentro de um modelo microeconômico de “principal e agente” (Jensen & Meckling, 1976), aonde os cidadãos são os “principais” e os servidores públicos são os “agentes”, que atuam e tomam decisões em nome dos cidadãos. Os servidores possuem informação assimétrica e poder discricionário sobre a alocação de recursos, o que possibilita a corrupção. Desta forma, as estratégias de combate à corrupção dentro do arcabouço principal-agente estão focadas em reduzir o poder discricionário dos servidores e melhorar o monitoramento, a transparência e a responsabilização.

A grande corrupção ocorre quando servidores ou agentes públicos subtraem de algum grupo social ou de parcela significativa da sociedade algum direito fundamental, ou causam perdas financeiras

4. <https://www.microsoft.com/en-us/microsoftacts/tackling-corruption-with-transparency-and-technology-part-1>

5. <https://www.icij.org/investigations/pandora-papers/>

substanciais ao estado ou aos cidadãos como resultado de corrupção. Nesse contexto a corrupção é definida como um problema de ação coletiva aonde diferentes grupos de atores que atuam no governo, no setor privado e na sociedade civil falham em se organizar em função do interesse coletivo. Em outras palavras, a grande corrupção é perpetrada pelos líderes corruptos que controlam as instituições do Estado, e que atuam para expropriar os recursos públicos em benefício próprio contando com a impunidade. Esse tipo de corrupção é notoriamente mais difícil de se combater com o uso das ferramentas de IA, uma vez que as próprias elites corruptas desenharam e controlam o sistema no qual elas operam. Nesse contexto, para o combate à grande corrupção as ferramentas que melhor se adequam são as que organizam ações coletivas de baixo para cima (“*bottom-up*”), por exemplo, identificando os agentes públicos suspeitos de corrupção ou enfraquecendo o monopólio da informação muitas vezes detido pelos agentes corruptos.

No Brasil, o robô “Rosie”, da operação Serenata de Amor<sup>6</sup>, é um exemplo concreto da utilização “*bottom-up*” da IA por parte da sociedade para monitorar o uso incorreto dos recursos públicos, automaticamente analisando as bases de dados de despesas de parlamentares em busca de gastos suspeitos. Na Nigéria, o projeto DataCrowd aplica a tecnologia de IA para permitir aos cidadãos o monitoramento contínuo dos projetos públicos e combater a corrupção.

Outras iniciativas anti-corrupção do ponto de vista “*bottom-up*” incluem a adoção de ações coletivas em caráter continuado, por parte dos cidadãos. As ferramentas de IA podem ajudar nesse sentido de várias formas. Os robôs de *Chatbot* podem ser úteis para receber denúncias por partes dos cidadãos, processando os dados recebidos de forma automática. Outra forma pode incluir a criação de robôs de IA desempenhando o papel de motivadores dos cidadãos e ajudando-os a se manterem mobilizados e engajados (Savage, Monroy & Hollerer, 2019), através de ativismo nas redes sociais (“*Botivism*”), como por exemplo, com o envio de mensagens personalizadas para cada cidadão, baseadas nas atividades anteriores de cada um. (Grau, Naderi & Kim, 2018).

Já do ponto de vista *Top-Down*, ou seja, iniciativas anti-corrupção adotadas parte dos entes gover-

namentais, o estudo recente de Darrel West (2021) pesquisador associado ao instituto não-governamental norte-americano de pesquisa de políticas públicas *Brookings Institution*, intitulado “*Using AI to Reduce Government Fraud*”, ilustra o amplo papel que a Inteligência Artificial pode desempenhar na redução da fraude governamental e também em diversas outras funções públicas.

Wirtz, Weyerer & Geyer (2018) citam que em particular a China e os Estados Unidos tem reconhecido o valor da IA para o setor público e também para a sua competitividade na economia global. Por exemplo, o Conselho de Estado da República Popular da China emitiu uma diretriz programando um investimento total de US\$ 147,8 bilhões para se tornar um inovador global na área de IA até 2030. (*State Council of the Peoples Republic of China*, 2017). O Estados Unidos também tem investido pesado na promoção de pesquisa para o desenvolvimento de tecnologias relacionadas a IA (Holdren & Smith, 2016). De forma similar, a Europa também vem investindo largas somas em robótica e parceria público-privada no contexto de IA. (Ansiip, 2017).

Lopez-Iturriaga & Sanz (2017) descrevem uma aplicação notável para a previsão de corrupção utilizando IA desenvolvida na Espanha na universidade de Valladolid, um sistema de alerta (*early warning*) baseado em uma rede neural e *Self-Organizing Maps (SOM)*. Os pesquisadores usaram dados da mídia e dados da justiça de casos de corrupção em várias províncias espanholas entre 2000 e 2012. Eles concluíram que a corrupção é estimulada pelos tributos cobrados sobre imóveis, crescimento econômico, aumento no preço dos imóveis, número crescente de instituições de financeiras e empresas não-financeiras, e o mesmo partido político permanecendo no poder por muito anos seguidos. Eles argumentam que seu modelo preditivo pode calcular a probabilidade de corrupção nas diferentes províncias e as condições que as favorecem, com até 3 anos de antecedência.

Entretanto, o uso de abordagens “*Top-Down*” contém riscos adicionais em relação à abordagem “*bottom-up*”. Por exemplo, em democracias frágeis ou autocracias, a utilização de sistemas de IA pelos governos poderá levar à consolidação de poder pelo governante de ocasião, desviando a IA de sua função original na direção dos objetivos de uma agenda personalista de poder, introduzindo desta

6. [www.serenata.ai](http://www.serenata.ai)

forma riscos adicionais de corrupção. O projeto “Zero Trust” introduzido pelo governo chinês para combater a corrupção de seus mais de 60 milhões de servidores públicos permite entendermos que, embora a IA possibilite cruzamento de dados e o cálculo de probabilidades de corrupção dos servidores, produz também uma concentração de poder. Isso tende a levar a diversos tipos de abusos, como no chamado efeito “Big Brother”, aonde os governos utilizam ferramentas de IA para monitorar e até mesmo perseguir a oposição política. (Laskowski, Johnson, Maillart & Chuang, 2014).

No Brasil, os sistemas de IA mais conhecidos em execução por órgãos de controle governamentais são os sistemas que utilizam os acrônimos ALICE, ADELE, MONICA e SOFIA do TCU (Odilla, 2021). O sistema ALICE, que significa Análise de Licitações e Editais, analisa automaticamente os editais de licitação e seus anexos em busca de não conformidades, emitindo alertas aos auditores. Já o sistema ADELE, Análise de Disputas em Licitações Eletrônicas, analisa os pregões eletrônicos, cruzando as informações das empresas participantes, por exemplo, quadro societário, ramo de atuação, e até a utilização do mesmo IP por empresas diferentes, buscando indícios de fraudes entre os licitantes. O sistema MONICA, Monitoramento Integrado para Controle de Aquisições, por sua vez traz informações sobre compras dos três Poderes da União, através de um painel interativo. E finalmente o SOFIA, Sistema de Orientação sobre Fatos e Indícios, ajuda o auditor na redação dos relatórios de auditoria, apontando possíveis erros, inclusive propondo a inclusão de informações relacionadas.

Em um artigo muito interessante, Neves, F. R., Da Silva, P. B., & Carvalho, H. L. M. de. (2019) reúnem evidências sobre a efetiva utilização dessas ferramentas citadas pelos auditores do TCU, revelando que seu uso ainda é baixo entre os técnicos do órgão.

## REGULAMENTAÇÃO E ÉTICA

Como vimos, as inúmeras aplicações baseadas em IA para o serviço público que estão surgindo trazem desafios importantes, que podem ser particularmente observados no que tange a responsabilidade e implementação da IA, bem como em temas éticos e sociais (Quraishi, Wajid & Dhiman, 2017,

Ransbotham, Kiron, Gebert & Reeves, 2017) que são ameaças potenciais ao uso bem-sucedido e respectiva criação de valor para o setor público e para a sociedade como um todo.

Com a evolução rápida dos riscos à segurança e privacidade relacionados ao uso da IA, os governos já começam a considerar uma forma de monitorar e responsabilizar as organizações que não identifiquem e administrem efetivamente esses riscos. Em 2021 a União Européia se tornou o primeiro órgão governamental dos países desenvolvidos a emitir um projeto de regulação<sup>7</sup> (“AI act”) visando especificamente o desenvolvimento e uso de IA.

No Brasil, o projeto de lei no 21 de 2020 ainda está tramitando no Senado Federal, e propõe estabelecer os fundamentos, princípios e diretrizes para o desenvolvimento e aplicação da IA no país. Elaborado por uma comissão de juristas, a proposta de regulação está baseada em critérios de avaliação de riscos e regras para avaliação do impacto algorítmico<sup>8</sup>. Com 18 integrantes, a comissão ouviu mais de 50 especialistas em audiências públicas e chegou a promover um seminário internacional. A maior parte das audiências discutiu os eixos temáticos do projeto: conceitos, compreensão e classificação de inteligência artificial; impactos da inteligência artificial; direitos e deveres; “accountability” (prestação de contas), governança e fiscalização.

A rigor, o tema de Ética da Inteligência Artificial suscita importantes dilemas em diversas áreas, tendo chamado a atenção também de órgãos multilaterais como a UNESCO<sup>9</sup> – agência especializada da ONU destinada a promover a paz e segurança mundiais através da cooperação na educação, artes, ciência e cultura.

Recentemente, os 193 Estados-membros da UNESCO assinaram o primeiro acordo global a respeito da Ética da Inteligência Artificial, na conferência geral da entidade, em novembro de 2021, tendo publicado o documento “Recommendation on the Ethics of Artificial Intelligence” - UNESCO (2022).

A Ética na utilização da IA, como também já foi dito anteriormente nesse artigo, é um dos pilares e

7. <https://artificialintelligenceact.eu/>

8. Fonte: Agência Senado. <https://www12.senado.leg.br/noticias/materias/2022/10/20/inteligencia-artificial-ja-tem-esboco-de-regulacao>

9. UNESCO – Organização das Nações Unidas para a Educação, a Ciência e a Cultura

princípios norteadores desse projeto no Município do Rio de Janeiro.

## INTELIGÊNCIA ARTIFICIAL E *MACHINE LEARNING* – ASPECTOS TÉCNICOS ESSENCIAIS

A Inteligência Artificial (IA) e o *Machine Learning* (ML) são termos frequentemente utilizados de forma intercambiável, mas são conceitos distintos. Enquanto a IA se refere ao desenvolvimento de sistemas capazes de realizar tarefas que normalmente requerem inteligência humana, como compreender linguagem natural e tomar decisões, o ML é uma subárea da IA que se concentra na criação de algoritmos capazes de aprender a partir de dados.

O ML é uma parte fundamental da IA, pois fornece a capacidade de aprendizado automático aos sistemas de IA. Ao contrário do desenvolvimento de sistemas de IA baseados em regras, onde o programador define regras específicas para uma tarefa, o ML permite que os sistemas aprendam a partir de exemplos e se ajustem automaticamente com base em novos dados.

Em resumo, a IA e o ML estão interligados, mas são conceitos distintos. A IA se refere ao desenvolvimento de sistemas inteligentes<sup>10</sup>, enquanto o ML se concentra na capacidade de aprendizado automático<sup>11</sup> desses sistemas. O ML é uma parte fundamental da IA, fornecendo a habilidade de aprender e se ajustar automaticamente a novos dados.

Para os interessados na história da evolução da área de Inteligência Artificial nas últimas décadas, Nilsson (2009) é uma referência interessante.

Explicaremos agora de forma técnica porém sucinta, o que é *Machine Learning*, que já definimos como uma subárea de Inteligência Artificial.

Para os autores Deisenroth, Faisal e Ong (2019), pode-se definir *Machine Learning* como o conjunto de métodos que podem detectar automaticamente padrões nos dados, e então utilizar esses padrões descobertos para prever dados futuros ou para realizar outros tipos de decisão sob incerteza. Existem diversos tipos de ML, incluindo o aprendizado supervisionado, o aprendizado não-supervisionado e o aprendizado por reforço.

Murphy (2012) ensina que no aprendizado supervisionado, o algoritmo de ML é alimentado com exemplos de treinamento “rotulados”, permitindo que ele aprenda a associar cada entrada específica a uma saída desejada. Nesta abordagem o objetivo do modelo estatístico é aprender um mapeamento das variáveis de entrada  $X$  para as variáveis de saída  $Y$ , dado um conjunto de pares identificados entrada-saída,  $D = \{(x_i, y_i)\}_{N_t}$ , aonde  $D$  é chamado de conjunto de treino, e  $N$  é o número de exemplos de treino. De forma simplificada, cada variável de entrada de treino  $X$  é um vetor  $D$ -dimensional de números, representando, por exemplo, a altura e o peso de uma pessoa. Essas características são chamadas de atributos. Em geral, contudo, essas variáveis  $X$  podem ser qualquer objeto de estrutura complexa, como uma imagem, uma forma molecular, um grafo, ou uma série de valores indexados ao tempo. Analogamente, a forma da variável de saída pode, a princípio, ser qualquer coisa, mas a maioria dos métodos de *Machine Learning* assume que  $y_i$  é uma variável categórica ou nominal de um conjunto finito  $y_i \in \{1, \dots, C\}$  ou que  $y_i$  seja um número do conjunto dos Reais. No primeiro caso, o problema é conhecido como de Classificação ou reconhecimento de padrões, e no segundo caso, o problema é conhecido como Regressão.

No aprendizado não supervisionado, o algoritmo é exposto a dados não rotulados e é responsável por encontrar padrões e agrupar os dados de forma significativa. O objetivo, portanto, é conseguir revelar alguma estrutura interessante no conjunto dos dados. Ao contrário da abordagem de aprendizado supervisionado, não há uma correspondência entre os dados de saída desejados (dados rotulados, na terminologia utilizada) para cada dado de entrada. Esta abordagem se assemelha mais ao processo de aprendizado típico dos seres humanos e dos animais, além de poder ser mais amplamente aplicada, pois não requer um “expert” que associe aos dados de entrada os dados de saída desejáveis ou “corretos”.

Finalmente, no aprendizado por reforço, o algoritmo é treinado por meio de uma recompensa ou punição para ações tomadas em um ambiente.

A seguir relatamos as principais etapas e desafios enfrentados no desenvolvimento dos sistemas de inteligência artificial para a detecção de fraudes na CGM-RJ, podendo servir como experiência para

10. Exemplos de sistemas de IA: Algoritmos genéticos, Busca Heurística, Redes Neurais profundas, algoritmos de grafos, etc.

11. Exemplos de modelos de ML: Regressão linear, regressão logística, árvores de decisão, Support Vector Machines, Modelos Bayesianos, etc.

as demais controladorias do Brasil que planejem desenvolver internamente este tipo de atividade.

## INTELIGÊNCIA ARTIFICIAL NA CORREGEDORIA DO MUNICÍPIO DO RIO DE JANEIRO

O projeto de desenvolvimento de IA na corregedoria é relativamente recente, tendo surgido apenas no início de 2021, a partir da iniciativa do coordenador técnico da corregedoria, da área de responsabilização de pessoas jurídicas, que constatou a necessidade do órgão de corregedoria de analisar um grande volume de dados, sendo muitos não-estruturados, com a finalidade de detecção de fraudes, irregularidades e demais atos ímprobos. A idéia do projeto foi comunicada ao subcontrolador de corregedoria e ao controlador geral do município, que apoiaram de imediato a iniciativa, tendo sido o projeto colocado como uma das metas estratégicas da controladoria.

Os anos de 2021 e 2022 foram dedicados inicialmente a desenhar as etapas de execução do projeto e definir os aspectos técnicos do algoritmo de detecção de corrupção. Para se chegar a etapa de estimação desse algoritmo e conseqüentemente iniciar a geração de sinais, é condição necessária a execução das etapas precedentes do processo, que são a obtenção de bases de dados íntegras, o cálculo das tipologias a partir dessas bases de dados, e a definição dos fatores de risco adicionais do sistema.

A etapa na qual o projeto se encontra no início de 2023 é a fase de cálculo das tipologias inicialmente definidas no planejamento e de determinação dos fatores de risco adicionais. Em seguida será iniciada a etapa de estimação do algoritmo de classificação para detecção de zonas de corrupção.

O objetivo final é construir uma poderosa ferramenta no trabalho analítico da Controladoria em

sua missão institucional, multiplicando o alcance da área de corregedoria no processo de detecção de fraudes e de atos de corrupção no município e otimizando a utilização de seus recursos humanos.

Veremos a seguir, de forma sequencial, as seguintes etapas:

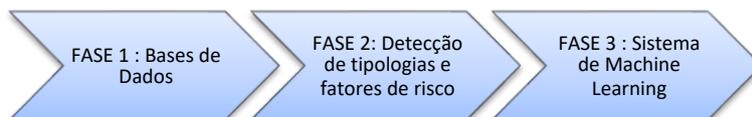
- a. Visão geral do projeto
- b. Seleção do *software* de desenvolvimento de algoritmos
- c. Definição do primeiro conjunto de análises (tipologias)
- d. Desenho dos processos de trabalho e *deployment*<sup>12</sup>

### A. VISÃO GERAL DO PROJETO

De forma bem ampla e abrangente, o projeto consiste, na Fase 1, em obter as bases de dados da prefeitura do Rio de Janeiro – bases de contratos, execução orçamentária e todas as outras necessárias, na Fase 2 utilizar essas bases para calcular as tipologias inicialmente definidas, e após identificar os demais fatores de risco de corrupção, construir uma nova base de dados contendo o histórico das tipologias, dos fatores de risco identificados e dos eventos de fraude/corrupção detectados historicamente nas Secretarias e Empresas Indiretas. Em seguida, na Fase 3, serão aplicadas as técnicas de Inteligência Artificial (*Machine Learning*) à essa nova base de dados para se estimar os parâmetros do sistema de detecção, e se iniciar efetivamente o monitoramento contínuo das informações, visando detectar situações de alto risco de corrupção, em tempo real ou com pouca defasagem. O projeto se encontra atualmente no desenvolvimento da Fase 2.

12. Entrega dos resultados dos algoritmos já em produção

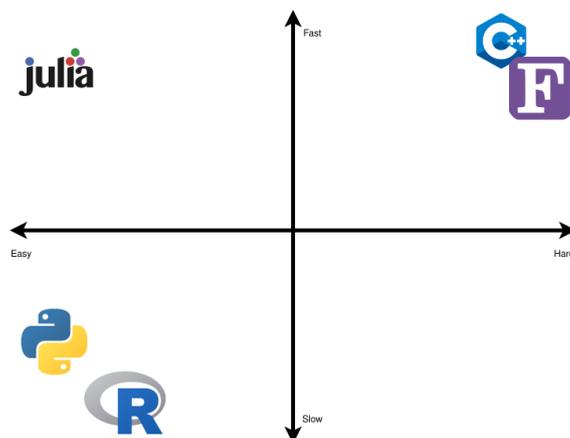
FIGURA 01: FLUXO DE ETAPAS DO PROJETO



## B. SELEÇÃO DO SOFTWARE DE DESENVOLVIMENTO DE ALGORITMOS

Inicialmente a escolha do software recaiu sobre duas possibilidades, sendo ambas de licença aberta<sup>13</sup> e de amplo uso para análise estatística de dados em grande volume, sendo elas a linguagem Python<sup>14</sup> e o software estatístico R<sup>15</sup>. Recentemente uma terceira opção tem sido considerada pela equipe, também com licença aberta, que é a utilização da linguagem científica Julia<sup>16</sup>. O diagrama a seguir mostra que a linguagem Julia está posicionada em um nicho específico que contém vantagens importantes em projetos intensivos em análise de dados. No eixo X as linguagens de programação estão ordenadas pela relativa facilidade de aprendizado e clareza da sintaxe. No eixo Y estão ordenadas pelo desempenho, do mais lento para o mais rápido. Julia consegue ser uma linguagem relativamente fácil de se aprender/utilizar, mantendo uma performance similar a C++, com a desvantagem de ser relativamente mais nova do que as outras.

FIGURA 02: COMPARAÇÃO ENTRE AS LINGUAGENS DE PROGRAMAÇÃO



13. Software criado de forma colaborativa que dá ao usuário liberdade completa de utilização

14. Python - <https://www.python.org/>

15. Software R - <https://www.r-project.org/>

16. Julia - <https://www.julialang.org/>



TABELA 1: RESUMO DAS TIPOLOGIAS

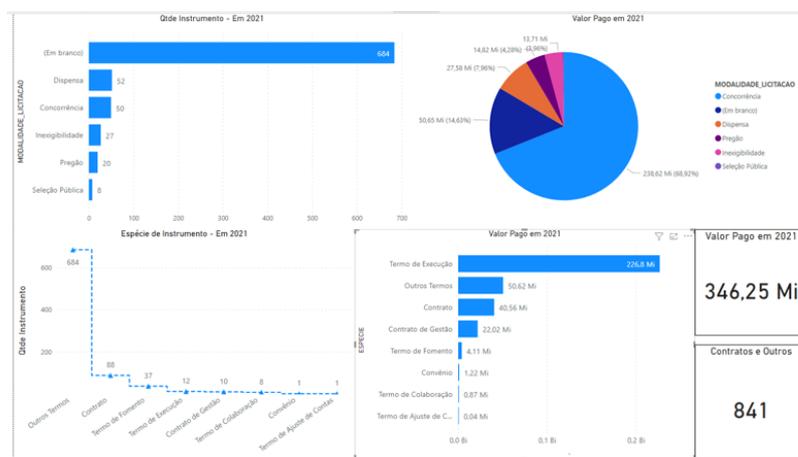
TIPOLOGIA	RESUMO	STATUS ATUAL
1. Execução físico-financeira do instrumento jurídico.	Apontar o descompasso entre a execução de serviço e seus respectivos pagamentos de despesas	Protótipo concluído. Primeira revisão pela área técnica concluída. Homologado.
2. Despesas realizadas após o encerramento do instrumento jurídico.	Despesas que, embora possuam instrumento jurídico, foram pagas a seus respectivos favorecidos a partir de empenhos com data posterior à data de encerramento.	Protótipo concluído. Primeira revisão pela área técnica levantou algumas exceções que estão sendo analisadas. Não-homologado.
3. Preços muito acima da média praticada pelo Município do RJ	Compras por valores injustificadamente altos	Protótipo em desenvolvimento. Não revisado pela área técnica. Não-homologado.
4. Identificação de adesão irregular à ata de registro de preços	Adesão irregular de entes da administração direta em atas de registros de preços sob a gestão de entes da administração indireta (e vice-versa)	Protótipo em desenvolvimento. Não revisado pela área técnica. Não-homologado.
5. Despesas sem Empenho	Visa a identificação de despesas municipais sem prévio empenho.	Protótipo em desenvolvimento. Não revisado pela área técnica. Não-homologado.

A escolha das tipologias seguiu os princípios da simplicidade e objetividade. Embora análises mais complexas possam ser necessárias em momento futuro, a opção foi iniciar pelas mais simples, porém não menos importantes, que são descritas de forma sucinta a seguir, incluindo exemplos de visualização (com dados hipotéticos para exemplificar) implementados em PowerBI:

#### Tipologia 01: Execução físico-financeira do instrumento jurídico.

O objetivo dessa tipologia é apontar o descompasso entre a execução de serviço e seus respectivos pagamentos de despesas, de acordo com o instrumento jurídico, a partir de um cronograma previsto em contrato, sugerindo a probabilidade de fraude na execução contratual.

FIGURA 04: EXEMPLO DE RESULTADO OBTIDO NA TIPOLOGIA 01



### Tipologia 02: Despesas realizadas após o encerramento do instrumento jurídico.

O objetivo dessa tipologia é identificar despesas que, embora possuam instrumento jurídico, foram pagas a seus respectivos favorecidos a partir de empenhos com data posterior à data de encerramento do vínculo desses instrumentos (incluindo seus aditivos), sugerindo a possibilidade de irregularidade ou fraude.

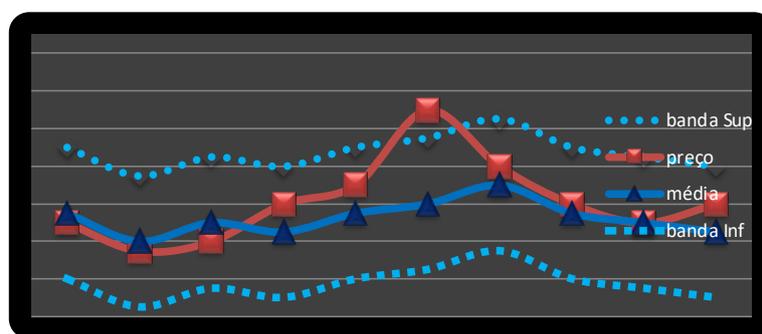
FIGURA 05 : EXEMPLO DE RESULTADO OBTIDO NA TIPOLOGIA 02



### Tipologia 03: Preços muito acima da média praticada pelo Município do RJ

O objetivo dessa tipologia é identificar a aquisição de produtos<sup>17</sup> pelas diferentes secretarias e empresas da administração indireta, detectando compras por valores injustificadamente altos<sup>18</sup>. Em um futuro desdobramento desta tipologia e ampliação do escopo deste projeto de IA, os algoritmos de *Machine Learning* poderão ser utilizados também para detectar padrões de comportamento entre fornecedores desses produtos, sinalizando a probabilidade de irregularidades, fraudes e conluios ou cartéis.

FIGURA 06: EXEMPLO DE ALERTA DE PREÇO GERADO PELA TIPOLOGIA 03.



O preço de aquisição de um item por uma Secretaria no quarto trimestre de 2020 situou-se acima do limite superior, considerando-se todas as compras realizadas deste item, neste mesmo trimestre, pela administração pública municipal.

17. Cada produto possui uma codificação específica válida para toda a prefeitura do RJ

18. Será definido um valor percentual acima da média como linha de corte, ou “banda superior” para sinalizar os preços acima do tolerável.

Além dessas, outras tipologias já planejadas são a **identificação de adesão irregular à ata de registro de preços** (tipologia 04), que busca identificar a adesão irregular de entes da administração direta em atas de registros de preços sob a gestão de entes da administração indireta (e vice-versa) para a aquisição de produtos ou prestação de serviços no âmbito do Município do RJ, e também uma tipologia para **identificação de despesas municipais sem prévio empenho** (tipologia 05).

#### **D. DESENHO DOS PROCESSOS DE TRABALHO E DEPLOYMENT/ VISUALIZAÇÃO**

No presente estágio do projeto ainda está em fase de definição o desenho do processo de trabalho, com escolhas definitivas a serem feitas a respeito da frequência de atualização dos algoritmos – a princípio a decisão preliminar é a estimativa a cada trimestre - e a respeito das permissões aos clientes internos dos relatórios, bem como de toda a rotina investigatória que será executada pela corregedoria após a detecção pelos algoritmos de *Machine Learning*, de sinais a respeito de provável corrupção e demais irregularidades.

Quanto ao *deployment* dos algoritmos, também ainda estão sendo definidas as melhores mídias em caráter definitivo. Além dos Relatórios de Inteligência em Word com a descrição dos achados de cada tipologia e do sistema de IA, também será utilizado o software PowerBI<sup>19</sup>. Está em avaliação também uma solução integrada com o software R utilizando o pacote RShiny<sup>20</sup>.

#### **DETECTANDO FRAUDE E CORRUPÇÃO COM MACHINE LEARNING**

Um algoritmo aprende com os dados se a performance em uma dada tarefa melhora após os dados terem sido levados em conta de forma objetiva. Desta forma quando utilizamos o aprendizado de máquina para detectar automaticamente padrões e estrutura nos dados, o que desejamos é encontrar bons modelos que generalizem suficientemente bem para dados ainda desconhecidos, ou seja, que obtenha resultados consistentes fora da amostra utilizada.

Em um dos processos de trabalho que está sendo desenvolvido na corregedoria, quando ocorrer uma previsão pelo algoritmo de *Machine Learning* de uma situação de alto risco de fraude ou corrupção, deverá ser designada uma equipe especial para analisar de forma aprofundada os contratos e as transações em questão, bem como para investigar outras despesas e contratos correlacionados à estas, além de uma amostra aleatória de transações deste órgão no período em questão. Neste processo, portanto, a corregedoria utilizará a tecnologia de Inteligência Artificial de forma a otimizar a utilização de recursos limitados e escassos (no caso, o tempo de trabalho da equipe super-especializada) no combate à fraude e corrupção, sem prejuízo das demais atividades realizadas pelas auditorias rotineiras;

Vamos descrever a seguir em maiores detalhes, mas de forma breve, os requisitos técnicos necessários da etapa final, na qual será executado o algoritmo de detecção de corrupção que está no centro deste projeto.

Inicialmente será necessária a criação de uma nova base de dados, consolidada com os valores históricos das tipologias calculadas nas frequências de tempo escolhidas, para todo o período disponível. No caso do Município do Rio de Janeiro esta frequência será inicialmente trimestral, e a base de dados existente corresponde aos últimos 22 anos de transações. A utilização de 22 anos de dados históricos reflete a intenção de usar como data de corte o ano 2000, quando as bases de dados já estavam bastante consolidadas e íntegras no município. Além das cinco tipologias calculadas conforme descrito em seção anterior deste artigo, serão criadas também séries históricas de outros fatores de risco que, na análise da equipe do projeto, se possa inferir *a priori* que possuam correlação com uma alta possibilidade de corrupção e fraude. Um exemplo é a existência de períodos atípicos de gastos públicos (como o período de uma Copa do Mundo, Olimpíada, ou de uma pandemia como a COVID-19, por exemplo), ou outras situações que fujam ao padrão de normalidade esperada no comportamento das transações públicas. Estes fatores de risco obviamente são específicos para cada unidade da federação e para cada ente público, podendo ser construídos tanto de forma binária, assumindo valores 0 ou 1 para a ativação ou não do risco naquele período, ou assumindo valores numa escala pré-definida pelo

19. <https://powerbi.microsoft.com/pt-br/>

20. <https://shiny.rstudio.com/>

usuário. Iremos denominar as variáveis relativas às tipologias de “TIP1” a “TIP5” e para os fatores de risco identificados “FR1” a “FR3”, assumindo que foram identificados 3 fatores de risco de interesse, construídos de forma binária, a título de exemplo.

Além de uma base de dados organizada com a série histórica destas variáveis, é essencial que se tenha também uma série histórica dos casos de fraudes e corrupção. Esta talvez seja a base de dados mais difícil de se obter, devendo na maioria

dos casos ser construída pela própria equipe do projeto, em um processo de pesquisa em múltiplas fontes, que muitas vezes pode ser trabalhoso e dificultoso. Por isso é essencial também o apoio total da alta gestão a um projeto desta natureza.

Para uma amostra com “N” observações no tempo e “S” Unidades Orçamentárias ou Secretarias, a tabela de dados final que será utilizada pelo algoritmo de *Machine Learning* terá uma estrutura similar ao exemplo hipotético a seguir:

**TABELA 2: DADOS HIPOTÉTICOS, COM TOTAL DE “N” TRIMESTRES E “S” SECRETARIAS**

OBSERVAÇÃO	TIP1	TIP2	TIP3	TIP4	TIP5	FR1	FR2	FR3	CORRUPÇÃO DETECTADA
n=1, s=1	0	0	0	123	123	0	0	0	Negativo
n=2, s=1	123	123	0	123	0	0	123	0	Positivo
n=3, s=1	123	0	0	123	0	0	123	0	Positivo
n=4, s=1	0	123	0	0	123	0	123	0	Negativo
n=5, s=1	0	123	0	123	0	0	0	0	Negativo
...	...	...	...	...	...	...	...	...	...
n=N, s=S	TIP1N,S	TIP2N,S	TIP3N,S	TIP4N,S	TIP5N,S	FR1N,S	FR2N,S	FR3N,S	DETECTN,S

Aonde em cada coluna “TIP” de 1 a 5 se tem a série histórica do número de casos detectados na referida tipologia por Secretaria “S” em cada um dos trimestres “N”. A coluna FR registra se houve ou não ocorrência de algum Fator de Risco “FR” 1 a 3, naquele mesmo trimestre, e finalmente a coluna “Corrupção Detectada”, registra se houve ou não detecção de fraude naquela Secretaria no trimestre.

Pode-se estimar o modelo utilizando um ou mais algoritmos, sendo importante separar a base de dados em dados de treino, que serão utilizados para estimar os parâmetros do modelo, e base de dados de teste, em que se analisará a performance do algoritmo.

Dentre os algoritmos de *Machine Learning* que podem ser utilizados para prever a ocorrência de corrupção, estão algoritmos de classificação como RandomForest (pacotes do software R, “randomForest” ou “rpart”, por exemplo, com licença gratuita), e Support Vector machine (pode-se utilizar o pacote “e1071” no R), dentre outros.

## DESAFIOS, LIMITAÇÕES E RESULTADOS PRELIMINARES

Como este projeto ainda está em desenvolvimento, está será uma análise não exaustiva do que foi encontrado até o momento, sujeita a revisões futuras e atualizações.

Um dos desafios mais relevantes de qualquer projeto de IA com certeza reside nas bases de dados que são utilizadas. Este aspecto desafiador foi citado em diversos trabalhos na seção anterior de revisão da literatura, como Wirtz, Weyerer & Geyer (2018) e Kobis, Starke & Rahwan, (2022). Mesmo contando com o apoio de servidores experientes e com uma base de dados com manutenção adequada, foi necessário algum tempo até nos certificarmos de que alguns tipos de informações constantes em alguns campos da base realmente correspondiam aquilo que precisávamos. Ou seja, foi feito um procedimento intensivo de *data cleaning*. Em alguns casos, foi necessário solicitar uma nova extração de arquivo de dados, contendo algumas informações necessárias ao projeto que, apesar de constarem da base de dados, não possuíam acesso fácil por não

serem utilizadas com muita frequência em relatórios usuais do órgão.

É importante registrar o grande ataque hacker sofrido pelo município do Rio de Janeiro em agosto de 2022, amplamente divulgado na imprensa, que atrasou consideravelmente a continuidade do projeto de IA da Controladoria, em função de uma série de restrições e protocolos emergenciais de segurança que foram adotados pela administração municipal, durante pelo menos 4 meses. Esse evento acendeu um sinal de alerta importante no que diz respeito à segurança das informações de todo o município e também do projeto de IA que está sendo desenvolvido na Controladoria.

Ainda com relação à base de dados, um desafio relevante que o projeto enfrenta é a construção da série histórica de eventos de corrupção ocorridos no município, um conjunto de dados absolutamente crucial para se estimar o algoritmo de classificação, sendo esta uma tarefa que demanda um trabalho minucioso e relativamente lento de pesquisa, tanto de fontes internas – investigações preliminares, sindicâncias, dados sigilosos de servidores sancionados e demitidos, quanto de fontes externas, tais como relatórios de investigação de outros órgãos e tribunais, processos judiciais, além de reportagens em diversas mídias.

Como importante limitação global do projeto de IA na CGM-RJ, sabemos que na maior parte dos casos, o que é mais provável de ser detectado pelo algoritmo de IA é a chamada “corrupção pequena”, como definido por Adam & Fazekas (2021) e discutido na seção anterior de “Evidências”. Isto não deixa de ser um tanto quanto frustrante para os envolvidos no projeto, pois os maiores danos à sociedade efetivamente ocorrem no contexto da grande corrupção, muitas vezes associada a agentes políticos. Uma possível forma de mitigar um pouco esse problema está na utilização combinada de outras ferramentas de IA complementares à que está sendo desenvolvida atualmente na CGM-RJ. Por exemplo, ferramentas de análise de licitações e editais, na mesma linha do ALICE já citado anteriormente, e outras ferramentas de análise de risco em diferentes tipos de contratos, convênios, etc.

Porém, mesmo com a ampliação dos instrumentos tecnológicos de análise e detecção, as controladorias, por serem órgãos de Controle Interno e fazerem parte da estrutura do poder executivo, sempre terão um grau de autonomia menor do que os Tribunais que realizam o Controle Externo, estando mais sujeitas a sofrer pressão do governante de ocasião, em particular em entes federativos de menor orçamento e visibilidade nacional.

A discussão sobre ética, presente na seção anterior de revisão da literatura, no artigo de Wirtz, Weyerer & Geyer (2018), e de Kobis, Starke & Rahwan, (2022) também é um desafio importante que está presente no projeto da CGM-RJ. Um dos pontos mais importantes a esse respeito é a questão do tratamento de dados sigilosos. Apesar de preocupante, neste particular estamos otimistas em razão de estarmos enxergando muitas sinergias com o esforço de adequação que já vem sendo realizado nos processos da controladoria e de todo o município, em função da Lei Geral de Proteção de Dados.

Outro aspecto relevante está na dupla checagem, por um humano, das conclusões obtidas pelo algoritmo de IA. Isso é absolutamente essencial, devido à “corrupção” ser um tema sensível. De toda forma, no processo de trabalho que está sendo desenhado para a utilização do sistema de IA, os sinais detectados serão encaminhados para uma equipe especial de investigação que cumprirá determinados protocolos já utilizados pelos atuais auditores, garantindo o mesmo procedimento ético das auditorias realizadas pelo órgão.

Finalmente, embora seja uma avaliação prematura porque o projeto ainda não chegou na fase de estimação dos parâmetros do algoritmo de IA, em função de não termos ainda todas as cinco tipologias previstas já calculadas, e também ainda não termos a série histórica completa de eventos de corrupção nos órgãos municipais, as duas tipologias já estimadas apresentam resultados interessantes e em linha com o que esperávamos à luz de nosso conhecimento a posteriori das informações e da correlação dos resultados dessas tipologias com eventos de corrupção, o que sugere que a eficácia do algoritmo de IA na detecção de corrupção, até o presente momento, é promissora.

## CONCLUSÃO

A utilização de ferramentas de Inteligência Artificial para robustecer o combate às fraudes e irregularidades no setor público já é uma realidade em todo o mundo.

A ferramenta de IA em desenvolvimento pela CGM-RJ tem como característica utilizar uma base de dados construída com a série histórica de cinco tipologias e fatores de risco definidos *a priori*, como os dados de entrada de um algoritmo de *Machine Learning* do tipo supervisionado, que será utilizado para classificar, em tempo real e com frequência trimestral, cada Secretaria, cada empresa indireta e cada unidade orçamentária do Município do Rio de Janeiro em uma de duas classes possíveis: “baixo risco de corrupção” ou “alto risco de corrupção”. No evento da detecção de um sinal de alto risco de corrupção pelo algoritmo, uma série de procedimentos analíticos e investigatórios será iniciada por uma equipe especializada visando aprofundar a análise. Importante ressaltar que todo o processo conta com observância aos princípios da ética profissional, garantindo a proteção de dados sensíveis, e o respeito aos direitos humanos.

A execução desse projeto no Município do Rio de Janeiro permitirá o monitoramento e a análise de dados de forma muito mais eficiente, contribuindo

para a identificação de possíveis casos de corrupção e fraudes em tempo real. Outra vantagem da utilização da ferramenta de IA no combate à corrupção é a possibilidade de automatizar tarefas repetitivas, otimizando os processos de trabalho e liberando tempo para atividades mais estratégicas, como a investigação propriamente dita. Além disso, a utilização de tais tecnologias também pode ajudar a prevenir a corrupção, ao identificar padrões suspeitos de atividades ilegais antes que causem danos significativos.

No planejamento e execução deste projeto alguns pontos são de especial importância: as bases de dados utilizadas devem conter dados íntegros e confiáveis; a escolha da linguagem de programação a ser utilizada deve ser compatível com os objetivos do projeto; e ainda, é fundamental garantir o apoio da alta administração do órgão ao projeto, e observar os princípios éticos.

Por fim, embora ainda em fase de desenvolvimento, no atual estágio do projeto os resultados preliminares obtidos na estimativa das duas primeiras tipologias estão em linha com o esperado à luz da correlação dos resultados dessas tipologias com eventos de corrupção, o que classifica o desempenho esperado do algoritmo de IA em desenvolvimento pela CGM-RJ até o momento como promissor.

## REFERÊNCIAS

- Adam, Isabelle & Fazekas, Mihály (2021). **Are emerging technologies helping win the fight against corruption? A review of the state of evidence**. Information Economics and Policy.
- Aguilera, A., Barrera, R., & Gabriela, M. (2016). **Technological unemployment: An approximation to the Latin America case**. AD-minister,29,59-78
- Anderson M., & Anderson S.L.(2011). **Machine Ethics**. New York, NY: Cambridge University Press.
- Ansip, A. (2017). **Making the most of robotics and artificial intelligence in Europe**. Edited by European Commission.
- Barlett, S.J.(2017). **The case for government by artificial intelligence**. SSRN Journal, 1-15.
- Boyd, M. & Wilson, N. (2017). **Rapid developments in artificial intelligence: How might the New Zealand government respond?** Policy Quarterly, 13, 36-44
- Cath, C., Wachter, S., Mittelstadl, B., Taddeo, M., & Floridi,L.(2018). **Artificial Intelligence and the ‘good society’: The US, EU, and UK approach**. Science and Engineering ethics, 24, 505-528.
- Chen, H.(2009). **AI, E-government, and politics 2.0**. IEEE Intelligent Systems, 24, 64-86.

- Chou, J.S., Lin, C.W., Pham, A.D., Shao, J.Y. (2015). **Optimized artificial intelligence models for predicting project award price**. *Automation in Construction*, 54, 106-115.
- Deisenroth, Faisal e Ong (2020). **Mathematics for Machine Learning**. Cambridge University Press.
- Gasser, U. (2017). **AI and the law: Setting the stage**. Berkman Klein Center for Internet & Society at Harvard University.
- Grau, P., Naderi, B. & Kim, J. (2018). **Personalized Motivation-supportive messages for increasing participation in crowd-civic systems**. *Proceedings of the ACM on Human-Computer Interaction*. Vol 2, 1-22. Association for Computing Machinery, 2018.
- Holdren, J. & Smith, M. (2016). **Preparing for the future of artificial intelligence**. Edited by the Executive Office of the President National Science and Technology Council Committee on Technology. Washington, DC.
- Jensen, M. & Meckling, W. (1976). **The theory of the firm: Managerial behavior, agency costs and ownership structure**. *Journal of Financial Economics*, 3, 305-360.
- Johnson, D.G. (2015). **Technology with no human responsibility?** *Journal of Business Ethics*, 127, 707-715
- Johnson, D.G., Verdicchio, M. (2017). **AI Anxiety**. *Journal of the Association for Information Science and Technology*, 68, 2267-2270.
- Kobis, N., Starke, C. & Rahwan, I. (2022). **The promise and perils of using artificial intelligence to fight corruption**. *Nature Machine Intelligence*, 4, 418-424.
- Kouziokas, G. (2017). **The application of artificial intelligence in public administration for forecasting high crime risk transportation areas in urban environment**. *Transportation Research Procedia*, 24, 467-473
- Kouziokas, G., Chatzigeorgiou, A. & Perakis, K. (2017). **Artificial intelligence and regression analysis in predicting ground water levels in public administration**. *European Water Publications*, 57, 361-366
- Krausová, A. (2027). **Intersection between law and artificial intelligence**. *International Journal of Computer*, 27, 55-68.
- Laskowski, Paul, Johnson, B., Maillart, T. & Chuang, J. (2014). **Government Surveillance and Incentives to Abuse Power**. (2014).
- Lima, M.S.M., Delen, D. (2019). **Predicting and explaining corruption across countries: a Machine Learning approach**. *Government Information Quarterly*, 37.
- Lopez-Iturriaga, F.J., Sanz, I.P. (2017). **Predicting public corruption with neural networks: an analysis of Spanish provinces**. *Social Indicators Research*, 140, 975-998.
- Massaro, T.M., Norton, H.L., & Kaminski, M.E. (2017). **Siri-ously 2.0: What artificial intelligence reveals about the first amendment**. *Minnesota Law Review*, 179.
- Muller, V. (2014). **Risks of general artificial intelligence**. *Journal of Experimental & Theoretical Artificial Intelligence*, 26, 297-301
- Murphy, Kevin P. (2012). **Machine Learning a Probabilistic Perspective**. MIT Press.
- Neumann, Oliver, Guirguis Katharina & Steiner, Reto (2022). **Exploring artificial intelligence adoption in public organizations: a comparative case study**. *Public management Review*.
- Neves, F. R., Da Silva, P. B., & Carvalho, H. L. M. de. (2019). **Artificial Ladies against corruption: searching for legitimacy at the Brazilian Supreme Audit Institution**. *Revista de Contabilidade e Organizações*, 13(November), 31-50. <https://doi.org/10.11606 /issn.1982-6486.rco.2019.158530>

- Nilsson, Nils J. (2009). **The Quest for Artificial Intelligence: A History of Ideas and Achievements**. Cambridge University Press.
- Odilla, F. (2021). **Bots against corruption: Exploring benefits and limitations of AI-based anti-corruption technology**. ECPR Joint Sessions 2021 “Digital Media, *Machine Learning*, and Corruption: How the Newest Technological Development Facilitate and Curb Corruption Practices Across the World”. <https://ecpr.eu/Events/Event/PaperDetails/58190>
- Power, D.J. (2016). **“Big Brother” can watch us**. *Journal of Decision Systems*, 255. 578-588
- Quraishi, F., Wajid, S.A., & Dhiman, P. (2017). **Social and ethical impact of artificial intelligence on public: A case study of university students**. *International Journal of Scientific Research in Science, Engineering and Technology*, 3, 463-467
- Ransbotham, S. Kiron, D., Gerbert, P. & Reeves, M. (2017). **Reshaping business with artificial intelligence: Closing the gap between ambition and action**. Edited by MIT Sloan Management Review.
- Scherer, M.U. (2016). **Regulating artificial intelligence systems: Risks, challenges, competencies and strategies**. *Harvard Journal of Law & Technology*, 29, 353-400
- State Council of The People’s Republic of China (2017). **China issues guideline on artificial intelligence development**. 2018, recuperado de [http://english.www.gov.cn/policies/latest\\_releases/2017/07/20/content\\_281475742458322.htm](http://english.www.gov.cn/policies/latest_releases/2017/07/20/content_281475742458322.htm)
- Sun, T. & Medaglia, R. (2017). **Artificial intelligence and public healthcare service innovation: A service ecosystem perspective**. The 40th information systems research in Scandinavia, IRIS 2017. Haiden, Norway.
- Tang, A., & Wen, A. (2009). **An intelligent simulation system for earthquake disaster assessment**. *Computers & Geosciences*, 35, 871-879.
- Thierer, A., O’Sullivan Castillo, A. & Russell, R. (2017). **Artificial intelligence and public policy**. Mercatus research. Edited by Mercatus Center at George mason University.
- Turing, Alan (1950). **Computing machinery and intelligence**, *Mind* no49, pp 433-460
- United Nations Educational, Scientific and Cultural Organization. UNESCO (2022) **Recommendations on The Ethics of Artificial Intelligence**. Paris, recuperado de <https://unesdoc.unesco.org/ark:/48223/pf0000381137>
- Velasquez, M., Andre, C., Shanks, T., Meyer, M.J. (2010). **What is ethics?** Edited by Markkula Center for Applied Ethics, Santa Clara University.
- West, Darrel (2021, 10 de setembro). **Using AI to Reduce Government Fraud**. Recuperado de <https://www.brookings.edu/research/using-ai-and-machine-learning-to-reduce-government-fraud/>
- Wirtz, Bernd W., Weyerer, Jan C. & Geyer, Carolin (2018). **Artificial Intelligence and the Public Sector – Applications and Challenges**, *International Journal of Public Administration*.
- Zheng, Y., Han, Y., Cui, L., Miao, C., Leung, C., & Yang, Q. (2018). **SmarHS : An AI platform for improving government service provision**. The 13th AAAI Conference on Inovative Applications of Artificial Intelligence (IAAI-18)

**Dalton Henrique Mota Ibere Gilson**[dalton.ibere@rio.rj.gov.br](mailto:dalton.ibere@rio.rj.gov.br)

ORCID:

Servidor da Controladoria Geral do Município do Rio de Janeiro, ocupando o cargo de Coordenador-Técnico da Subcontroladoria de Corregedoria, além de membro do Conselho Fiscal de empresas públicas, tendo experiência prévia como consultor no setor privado. Graduado em Administração de Empresas pela PUC-RJ e em Ciências Contábeis, pós-graduado em Finanças e Mestre em Finanças e Economia pela EPGE, FGV –RJ. Também é professor de pós-graduação executiva em Finanças Corporativas da Fundação Getúlio Vargas, ministrando aulas ininterruptamente desde 2005.

**Gustavo de Avellar Bramili**[gustavo.bramili@rio.rj.gov.br](mailto:gustavo.bramili@rio.rj.gov.br)

ORCID:

Servidor da Controladoria Geral do Município do Rio de Janeiro desde 1992, tendo transitado por todos os níveis hierárquicos da Auditoria Geral da Controladoria Geral do Município do Rio, ocupando por 30 anos cargos de chefia. Ainda foi Coordenador Geral da Central 1746, Transparência Rio e Sistema Municipal de Ouvidoria, entre outras atividades desenvolvidas como gestor. Desde janeiro de 2021, ocupa o cargo de Controlador Geral da CGM-Rio. É graduado em Ciências Contábeis e pós-graduado em Auditoria e Controladoria, sendo ainda especializado em Auditoria de Programas, Processos e Projetos, já tendo exercido o cargo de professor universitário em cursos de Graduação e Pós-Graduação.