

Entre a Eficiência e a Proteção: Potencialidades das Decisões Automatizadas no Reconhecimento de Direitos por Órgãos Públicos

Anderson Sousa Batista Machado
Faculdade de Tecnologia
Departamento de Engenharia Elétrica
Universidade de Brasília
Brasília, Distrito Federal, Brasil
anderson.machado@aluno.unb.br

Demétrio Antônio da Silva Filho
Instituto de Física
Universidade de Brasília
Brasília, Distrito Federal, Brasil
dasf@unb.br

Abstract—The digital transformation of the Brazilian public sector has accelerated the adoption of automated systems for decision-making in administrative and judicial processes, driven by advancements in artificial intelligence. However, the delegation of complex decisions to algorithms raises significant ethical, legal, and operational concerns, creating a critical gap in literature regarding systemic risks and practical control mechanisms. This article examines the potentialities and impacts of automated decisions in the recognition of rights by Brazilian public bodies, focusing on operational limitations, fraud risks, and governance challenges. Through a critical literature review, documentary analysis, and case studies from national and international contexts, it is shown that decision automation, while promoting efficiency and standardization, generates systemic risks, weakens transparency, and may compromise fundamental rights. The study highlights the need for robust institutional safeguards, such as meaningful human oversight, algorithmic audits, and explainability mechanisms, to mitigate risks and ensure legitimacy. The results reinforce that the advancement of automation requires the integration of efficiency, rights protection, and accountability.

Index Terms—Automated Decision; Recognition of Rights; Governance; Transparency; Public Sector.

Resumo—A transformação digital do setor público brasileiro tem acelerado a adoção de sistemas automatizados para a tomada de decisão em processos administrativos e judiciais, impulsionada pelos avanços na inteligência artificial. No entanto, a delegação de decisões complexas a algoritmos suscita preocupações éticas, jurídicas e operacionais significativas, criando uma lacuna crítica na literatura em relação aos riscos sistêmicos e aos mecanismos práticos de controle. Este artigo analisa as potencialidades e os impactos das decisões automatizadas no reconhecimento de direitos por órgãos públicos brasileiros, com ênfase nas limitações operacionais, riscos de fraude e desafios de governança. A partir de revisão bibliográfica crítica, análise documental e estudo de casos nacionais e internacionais, evidencia-se que a automação decisória, embora promova ganhos de eficiência e padronização, acarreta riscos sistêmicos, fragiliza a transparência e pode comprometer direitos fundamentais. O trabalho destaca a necessidade de salvaguardas institucionais, como supervisão humana significativa, auditorias algorítmicas e teste de integridade de sistemas, para mitigar riscos e assegurar legitimidade das decisões. Os resultados reforçam que a evolução da automação no setor público exige integração entre eficiência e proteção de direitos.

Palavras-chave—Decisão Automatizada; Reconhecimento de Direitos; Governança; Transparência; Setor público.

I. INTRODUÇÃO

A transformação digital no setor público brasileiro tem acelerado a adoção de sistemas automatizados para tomada de decisão em processos administrativos, judiciais e de gestão de políticas públicas. Esse movimento decorre, em grande medida, da consolidação de uma agenda normativa e institucional voltada à desburocratização, à prestação digital de serviços, à interoperabilidade de bases de dados, à inovação administrativa e ao aumento da eficiência estatal, conforme previsto na Lei nº 14.129/2021, que institui princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública [1].

Em complemento a esse cenário normativo, a Lei Geral de

Proteção de Dados Pessoais (LGPD) reconhece expressamente a existência de decisões tomadas com base em tratamento automatizado de dados pessoais, evidenciando a crescente relevância jurídica da automação decisória tanto no setor público quanto no privado [2].

A expansão da automação está associada, em grande medida, ao desenvolvimento e à incorporação de sistemas baseados em inteligência artificial (IA). Embora nem toda decisão automatizada utilize IA, técnicas como aprendizado de máquina (*machine learning*), mineração de dados e reconhecimento de padrões têm ampliado significativamente a capacidade dos órgãos públicos de processar informações, identificar inconsistências, realizar classificações e apoiar pro-

cessos decisórios em larga escala.

A literatura nacional aponta que a inteligência artificial (IA) já se encontra presente em diferentes organizações públicas brasileiras, ainda que de forma heterogênea e condicionada às capacidades institucionais e tecnológicas de cada órgão.

Ao analisar esse panorama, Ribeiro e Segatto observam que as instituições públicas brasileiras têm adotado tecnologias e técnicas em IA, mas esse processo ainda é limitado a um grupo pequeno delas. As autoras acrescentam que essa disseminação ocorre de maneira desigual entre os entes federativos, o que pode estar associado às distintas capacidades de tecnologia da informação existentes no setor público [3].

Uma das áreas em que essa transformação se manifesta de forma mais evidente é a de processos administrativos. Nesse contexto, a automação vem sendo empregada em atividades como triagem de requerimentos, análise documental, cruzamento de bases de dados, fiscalização, controle de conformidade, gestão de filas, processamento de benefícios e identificação de inconsistências.

Entre os exemplos mais expressivos destaca-se o Instituto Nacional do Seguro Social (INSS). Segundo divulgação institucional, em maio de 2023, “o INSS atingiu a maior quantidade de requerimentos decididos de maneira automática, um recorde histórico desde a implantação da inteligência artificial na análise dos benefícios. Em termos percentuais, foram concluídos 42%, representando mais de 222 mil benefícios” [4].

A literatura especializada indica que essa expansão da automação no INSS está diretamente relacionada aos desafios de capacidade operacional enfrentados pela instituição. Carvalho afirma que “o problema atual do INSS e das agências públicas de atendimento de larga escala é atender um grande volume de serviço, com escassez de pessoal”, circunstância que favorece a adoção de tecnologias voltadas à tomada de decisão automatizada [5].

Nessa mesma linha, Oliveira registra que o INSS passou a utilizar ferramentas de processamento automático de benefícios com base em informações validadas no CNIS, buscando promover maior celeridade e economia na prestação dos serviços públicos [6]. Contudo, a literatura também destaca limitações relevantes desse modelo. Rocha e Oliveira observam que, embora a inteligência artificial tenha contribuído para a redução da fila de espera previdenciária, também ocasionou negativas automáticas sem adequada justificativa aos segurados, evidenciando a necessidade de supervisão humana em casos mais complexos [7].

Além da área previdenciária, experiências de automação também vêm sendo desenvolvidas em atividades de controle, auditoria e fiscalização. Nesse contexto, destaca-se a ferramenta ALICE, utilizada pela Controladoria-Geral da União e pelo Tribunal de Contas da União, cuja finalidade é a análise preventiva de licitações por meio do processamento de grandes volumes de dados e da identificação de indícios de irregularidades, fraudes e riscos em contratações públicas.

Os resultados obtidos por essa iniciativa reforçam o potencial dessas tecnologias para apoiar a administração pública.

Em estudo de caso sobre a solução, Menezes e Resende apontam que, entre 2017 e 2020, a ferramenta contribuiu para evitar a ocorrência de gastos potencialmente irregulares que alcançaram aproximadamente R\$ 291 milhões [8].

A expansão da inteligência artificial, contudo, não se restringe à esfera administrativa. No âmbito dos processos judiciais, essas tecnologias também vêm sendo incorporadas de maneira crescente, sobretudo em atividades de classificação processual, identificação de precedentes, triagem de recursos, agrupamento de demandas repetitivas, pesquisa jurisprudencial e gestão de acervos.

Esse avanço foi acompanhado pela construção de mecanismos institucionais de governança. O Conselho Nacional de Justiça (CNJ) editou a Resolução nº 332/2020, que estabelece parâmetros éticos, de transparência e de governança para a produção e o uso de inteligência artificial no Poder Judiciário, além de estruturar a Plataforma Sinapses como ambiente nacional para armazenamento, treinamento, distribuição e auditoria de modelos de IA [9].

Como reflexo desse processo de institucionalização, levantamento realizado no âmbito do Programa Justiça 4.0 identificou 140 projetos de inteligência artificial desenvolvidos ou em desenvolvimento nos tribunais e conselhos de justiça brasileiros em 2023 [10]. Entre as iniciativas mais conhecidas encontra-se o Projeto Victor, desenvolvido no Supremo Tribunal Federal.

A literatura apresenta o Sistema Victor como uma experiência emblemática de utilização de inteligência artificial no Poder Judiciário brasileiro, especialmente em razão de sua aplicação à gestão de grandes volumes processuais e à triagem de recursos extraordinários.

Valle, Fuentes i Gasó e Ajus destacam que a digitalização dos processos judiciais e a modernização dos sistemas dos tribunais impulsionaram o uso dessas tecnologias, particularmente nas cortes superiores. Segundo os autores, o Projeto Victor foi desenvolvido em parceria entre o STF e a Universidade de Brasília e possui como funções principais a separação dos documentos relevantes dos processos e a classificação dos recursos por temas de repercussão geral [11].

Paralelamente às experiências observadas nas esferas administrativa e judicial, a inteligência artificial também vem sendo empregada na formulação, implementação e monitoramento de políticas públicas. Nessa área, os sistemas automatizados são utilizados para apoiar o planejamento governamental, a focalização de beneficiários, a fiscalização da execução de programas, a detecção de inconsistências e a prevenção de fraudes.

A relevância desse fenômeno foi evidenciada pelo Tribunal de Contas da União, que identificou que 28% das organizações da Administração Pública Federal já utilizam alguma solução baseada em inteligência artificial. Entre os benefícios relatados estão o aumento da produtividade, a redução de custos e tempo de execução dos processos, a melhoria da alocação de recursos humanos e o aumento da confiabilidade das atividades desenvolvidas [12].

Em consonância com esses achados, a literatura nacional reconhece a inteligência artificial como instrumento de moder-

nização administrativa e de aprimoramento da gestão pública. Anastasia sustenta que essas tecnologias podem transformar os processos de análise e tomada de decisão relacionados ao controle de políticas públicas, ao possibilitar a automação de tarefas rotineiras, a identificação de padrões complexos e a projeção de tendências futuras [13].

De forma semelhante, Vasconcelos e Santos ressaltam que a inteligência artificial possui potencial para ampliar a eficiência, a transparência e a inovação nos processos governamentais, podendo atuar como importante indutor da modernização do setor público quando implementada de maneira responsável [14].

Um exemplo concreto dessa aplicação é o Sistema de Seleção Aduaneira por Aprendizado de Máquina (SISAM), utilizado pela Receita Federal do Brasil desde 2014 como ferramenta de apoio à fiscalização aduaneira. Conforme registra Lietz, o sistema analisa os itens constantes das declarações de importação registradas no país, identificando padrões associados a infrações aduaneiras e aperfeiçoando a seleção de operações para conferência fiscal [15].

Diante desse panorama, observa-se que a automação decisória já está presente em múltiplos campos da atuação estatal brasileira, abrangendo desde a concessão de benefícios previdenciários e o controle das contratações públicas até a gestão processual no Judiciário e a implementação de políticas públicas.

Impulsionada pelos avanços da inteligência artificial e das técnicas de aprendizado de máquina (*machine learning*), essa transformação promete ganhos significativos de eficiência, celeridade, padronização, redução de custos e ampliação da capacidade estatal de processamento de dados.

Não obstante esses avanços tecnológicos, a delegação total ou parcial de decisões, por vezes complexas, a sistemas algorítmicos suscita relevantes preocupações de ordem ética, jurídica e operacional, especialmente em contextos de elevado impacto social e econômico.

A literatura aponta que decisões automatizadas no setor público podem gerar riscos relacionados, dentre outros, à opacidade decisória, à reprodução de vieses, à dificuldade de explicação dos critérios adotados e à insuficiência de supervisão humana [16]–[18].

Assim, a incorporação crescente de tecnologias automatizadas pelo setor público exige uma compreensão não apenas de seu potencial de eficiência, celeridade e padronização, mas também de seus limites, riscos e implicações práticas para a transparência, a *accountability* e a proteção de direitos fundamentais.

Além disso, embora a automação decisória venha se expandindo no setor público, com sistemas algorítmicos apoiando — ou, em certos casos, substituindo — etapas relevantes do processo decisório, a produção científica sobre seus impactos práticos e riscos institucionais ainda se mostra incipiente.

Ribeiro e Segatto registram que há um crescente debate sobre a adoção de tecnologias de inteligência artificial (IA) no setor público, mas ressaltam que poucos estudos analisam as características associadas à adoção dessas tecnologias e que,

no contexto brasileiro, persiste uma lacuna de estudos que discutem a adoção da IA pelas instituições públicas [3].

Essa lacuna também se manifesta na literatura internacional. Rizk e Lindgren observam que organizações públicas utilizam cada vez mais decisões automatizadas para ganho de eficiência, mas que ainda são necessárias pesquisas sobre modelos híbridos humano-algoritmo, tipos de decisão e salvaguardas voltadas à transparência e à proteção de direitos [18].

À vista disso, quando se observa a produção acadêmica nacional, nota-se que, apesar do crescente interesse pelo tema da automação no setor público, a literatura brasileira revela uma lacuna crítica não apenas regulatória, no que se refere à Lei Geral de Proteção de Dados (LGPD), mas também na análise operacional e integrada dos impactos decorrentes de decisões fundamentadas exclusivamente em Sistemas de Decisão Automatizada (do inglês, *Automated Decision Systems* — ADS).

Observa-se, ainda, uma escassez significativa de estudos que abordem, de forma sistemática, os riscos de fraude nesses sistemas e as limitações práticas dos mecanismos de controle atualmente existentes nas instituições que deles fazem uso.

Adicionalmente, faltam estudos que se aprofundem na proposição de modelos de supervisão híbrida viáveis — nos quais a intervenção humana seja significativa e não meramente formal — capazes de equilibrar a busca por eficiência tecnológica com a proteção de direitos.

Esses modelos, como mostrado no referencial teórico, são essenciais para evitar que a delegação da atividade decisória produza decisões erradas ou injustas e, consequentemente, comprometa direitos fundamentais, amplie desigualdades e fragilize a legitimidade das decisões jurídicas e administrativas. Esse cenário exige o desenvolvimento de práticas de governança responsáveis que transitem da reação ao dano para a prevenção de erros e fraudes sistêmicas.

Diante desse panorama, este artigo tem como objetivo analisar as potencialidades e os impactos das decisões automatizadas no reconhecimento de direitos por órgãos públicos brasileiros, com ênfase em limitações operacionais e fraude, bem como propor diretrizes de governança que mitiguem os riscos identificados.

Dessa forma, este artigo oferece uma contribuição relevante ao debater a urgência de uma governança responsável na tomada de decisão automatizada no setor público brasileiro. E, ao integrar revisão bibliográfica crítica, exemplos de casos reais e a proposição de diretrizes operacionais, espera-se que este estudo possa contribuir, fornecendo subsídios para gestores públicos, formuladores de políticas públicas e órgãos de controle.

II. REFERENCIAL TEÓRICO

Nesse cenário, observa-se que a literatura internacional tem se concentrado na análise dos benefícios e dos potenciais riscos associados à Tomada de Decisão Automatizada (do inglês, *Automated Decision-Making* — ADM) por Sistemas de Decisão Automatizada (do inglês, *Automated Decision Systems* — ADS).

Nesse contexto, a literatura distingue esses sistemas em **Sistemas de Decisão Totalmente Automatizada** (do inglês, *Fully Automated Decision Systems* — FADS), nos quais o algoritmo emite a decisão final sem qualquer intervenção humana, unicamente com base no tratamento automatizado de dados, e **Sistemas Automatizados de Suporte à Decisão** (do inglês, *Automated Decision Support Systems* — ADSS), que fornecem recomendações ou decisões que precisam ser referendadas por um *agente humano*, responsável último pelo julgamento. Essa diferenciação é central para compreender tanto os ganhos de eficiência e precisão quanto os riscos associados à delegação de decisões a algoritmos.

De forma crítica, a literatura enfatiza um conjunto de preocupações centrais relacionadas à Tomada de Decisão Automatizada. Entre elas, destacam-se a **opacidade decisória**, isto é, a dificuldade ou mesmo impossibilidade de compreender os critérios pelos quais um sistema algorítmico chega a uma determinada decisão ou recomendação; a possibilidade de **vieses discriminatórios**, decorrentes do risco de que algoritmos reproduzam ou amplifiquem desigualdades sociais já presentes nos dados de treinamento; e a **redução ou ausência de supervisão humana**, especialmente em sistemas de decisão totalmente automatizados. Tais preocupações reforçam a necessidade de mecanismos robustos de responsabilização algorítmica (*algorithmic accountability*) e de governança, capazes de assegurar transparência, rastreabilidade e legitimidade nos processos decisórios mediados por algoritmos.

Em termos práticos, no setor da saúde, a Tomada de Decisão Automatizada (ADM) manifesta-se principalmente por meio dos Sistemas de Suporte à Decisão Clínica (Clinical Decision Support Systems — CDSS). Esses sistemas têm demonstrado potencial para aprimorar a precisão e a eficiência de diagnósticos e prognósticos, sobretudo ao oferecer suporte aos profissionais de saúde por meio de alertas, lembretes e diretrizes clínicas incorporados aos fluxos de trabalho.

Sutton et al. (2020) [19] destacam que os alertas gerados por CDSS estão entre as formas mais difundidas de suporte à decisão clínica, contribuindo para orientar condutas, reduzir omissões e favorecer a adesão a boas práticas. Além disso, os autores apontam que esses sistemas também podem fortalecer a tomada de decisão compartilhada entre paciente e profissional de saúde, na medida em que ampliam o acesso à informação relevante e reduzem barreiras informacionais que dificultam a participação do paciente no próprio cuidado.

Disso, pode-se inferir que os CDSS são sistemas automatizados de suporte à decisão (ADSS) que atuam como ferramenta de integração e qualificação do processo decisório em saúde, ao fornecer suporte baseado em evidências que não apenas aprimora a prática clínica, mas também promove a participação ativa do paciente.

Os CDSS funcionam como mediadores entre dados clínicos, protocolos médicos e experiência profissional, contribuindo para a redução de incertezas diagnósticas e a padronização de tratamentos, além de fortalecer tanto a qualidade quanto a legitimidade das decisões clínicas, ao tornarem estas decisões mais justificáveis e transparentes, e envolverem o paciente no

processo.

Sob outro prisma, na segurança pública, a Tomada de Decisão Automatizada (ADM) tem se consolidado como uma das principais frentes de aplicação, voltada tanto para otimizar a alocação de recursos quanto para aprimorar a detecção de atividades anômalas em tempo real.

No Brasil, experiências recentes incluem o uso de modelos de policiamento preditivo, já testados em estados como São Paulo e Rio de Janeiro, para orientar o patrulhamento ostensivo com base em padrões históricos de criminalidade; a implementação de sistemas de reconhecimento facial, na Bahia e no Rio de Janeiro, empregados na identificação de foragidos e desaparecidos em grandes eventos e áreas de transporte público [20]; e a adoção de sistema de despacho assistido por computador (do inglês, *Computer Aided Dispatch* — CAD), sistema de decisão totalmente automatizada, como o Sinesp CAD do Ministério da Justiça e Segurança Pública (MJSP), que processam chamadas de emergência e definem automaticamente a viatura mais adequada para o atendimento.

Em corroboração, Castelluccia e Le Métayer [21] observam que diversas cidades já recorrem a Sistemas de Decisão Algorítmica (ADS) para fins de segurança pública, com a adoção de câmeras de vigilância com reconhecimento facial, drones e ferramentas de policiamento preditivo. Essas tecnologias, segundo os autores, ajudam a polícia a direcionar suas ações, definir prioridades operacionais e solucionar casos criminais [21].

Os mesmos autores, contudo, ressaltam que esses sistemas também apresentam riscos relevantes à privacidade, pois tecnologias de vigilância podem se tornar opressivas e invasivas, além de ampliar preconceitos, reforçar estigmatizações e gerar impactos desproporcionais sobre os cidadãos [21].

Guardadas as ressalvas necessárias, esses exemplos demonstram como a Tomada de Decisão Automatizada (ADM), ao integrar análise preditiva e monitoramento contínuo, vem transformando práticas operacionais e ampliando a capacidade de resposta das instituições de segurança pública no Brasil e no mundo.

Já na gestão tributária, a ADM é crucial para o aprimoramento da conformidade fiscal e para o aumento da eficiência da arrecadação. Como observam Rahman et al. (2024) [22], a ADM com auxílio de IA pode acelerar a classificação de contribuintes, verificar a consistência dos dados das declarações, detectar fraudes potenciais e melhorar estratégias de cobrança ao automatizar processos intensivos em mão de obra, reduzindo dessa forma custos operacionais e permitindo decisões mais bem fundamentadas.

Além disso, os autores complementam que o uso de algoritmos avançados e sistemas automatizados torna os processos de avaliação mais ágeis, minimizando os erros e assegurando que os contribuintes cumpram suas obrigações sem encargos desnecessários [22].

No cenário brasileiro, essa lógica de eficiência pode ser observada na Malha Fiscal Digital (MFD), instrumento utilizado pela Secretaria Especial da Receita Federal do Brasil (RFB) em ações de conformidade tributária. A MFD opera mediante

análise e cruzamento eletrônico de informações declaradas pelos contribuintes e de dados disponíveis à administração tributária, com o objetivo de estimular a regularização espontânea das divergências identificadas [23].

Apesar desses benefícios, há alerta na literatura para riscos importantes. Segundo Sever [16], a ADM apresenta diversos benefícios, como aumento da eficiência, redução de custos, consistência e decisões baseadas em dados. Entretanto, riscos, desafios e preocupações éticas devem também ser levados em conta: como a privacidade de dados, os vieses algorítmicos e as lacunas de capacitação.

Na mesma direção, em revisão multidisciplinar sobre a ADM no setor público, Rizk e Lindgren [18] destacam que a Tomada de Decisão Automatizada pode comprometer a legitimidade das organizações públicas caso não seja cuidadosamente concebida para preservar valores públicos relevantes.

Além disso, os autores defendem a necessidade de salvaguardas preventivas capazes de proteger direitos individuais e, simultaneamente, assegurar o interesse público em transparência [18]. Mais ainda, os autores chamam atenção para a adoção de sistemas híbridos de ADM no setor público, nos quais tanto humanos quanto algoritmos exercem agência decisória, ressaltando que tais modelos devem ser desenvolvidos de modo a minimizar vieses e preservar valores públicos fundamentais [18].

Sobre esse último conceito, os sistemas híbridos não devem ser confundidos com os sistemas automatizados de suporte à decisão (ADSS), ainda que ambos compartilhem a premissa de que o humano permanece envolvido no processo decisório.

Diferentemente dos ADSS, nos quais o algoritmo apenas sugere, classifica ou recomenda, cabendo ao humano a decisão final, os sistemas híbridos configuram um modelo de divisão de competências, em que humanos e algoritmos exercem poder decisório em seus respectivos escopos. Trata-se de uma arquitetura na qual a máquina não se limita a auxiliar, mas efetivamente decide determinadas etapas objetivas e padronizadas, enquanto o humano atua nas situações que demandam interpretação contextual, sensibilidade social ou análise de exceções.

Para além desses aspectos, a adoção de sistemas automatizados para a tomada de decisão em serviços públicos — seja em etapas específicas, seja em todo o processo decisório — acarreta riscos significativos de falhas sistêmicas, com potenciais repercussões financeiras, sociais e institucionais, além de prejuízos à credibilidade das organizações governamentais.

Nesse contexto, Rinta-Kahila et al. (2024) [24] examinaram o emblemático caso Robodebt, ocorrido na Austrália, que consistiu na implementação de um sistema automatizado para a cobrança de débitos relacionados a benefícios sociais. Esse sistema, segundo os autores, gerou notificações de dívida imprecisas e baseadas em evidências insuficientes. Como consequência, foram emitidas milhares de notificações indevidas a cidadãos australianos, evidenciando deficiências substanciais de governança algorítmica e suscitando relevantes debates éticos sobre a aplicação da automação na formulação e execução de políticas públicas.

A complexidade e os impactos do caso foram retratados na série televisiva *The People vs Robodebt* e no livro premiado de Rick Morton, intitulado “*Mean Streak: A moral vacuum, a dodgy debt generator and a multi-billion-dollar government shake down — the powerful story of robodebt*” [25]. O caso constitui, assim, um exemplo expressivo de como a automação mal governada pode produzir decisões indevidas, com impactos sociais significativos e perda de confiança nas instituições públicas.

Sob a perspectiva jurídico-regulatória comparada, ao contrastar Brasil e União Europeia, Toniazzi et al. (2021) [17] concluem que há uma diferença relevante entre os dois regimes de proteção. Na União Europeia, a decisão baseada unicamente no tratamento automatizado de dados é tratada, em regra, como prática vedada, assegurando-se ao titular o direito de não se submeter a esse tipo de decisão. No Brasil, por outro lado, a LGPD reconhece o direito à revisão da decisão automatizada, mas não garante expressamente que essa revisão seja realizada por uma pessoa humana.

Em síntese, o GDPR — Regulamento Geral de Proteção de Dados da União Europeia — parte da vedação à decisão exclusivamente automatizada, admitindo-a apenas em hipóteses excepcionais e mediante salvaguardas, entre elas o direito à intervenção humana.

Já o modelo brasileiro, previsto na LGPD, concentra-se no direito posterior de revisão da decisão automatizada, sem assegurar expressamente que essa revisão seja realizada por uma pessoa humana, o que representa uma lacuna relevante na proteção jurídica dos titulares de dados.

Ademais, Toniazzi et al. (2021) [17] sustentam que a legitimidade da decisão automatizada depende de sua explicabilidade e da preservação da intervenção humana. Para os autores, a decisão deve ser compreensível tanto quanto à lógica utilizada pelo sistema quanto em relação aos fundamentos que justificam o resultado produzido. Nessa perspectiva, a exclusão do elemento humano da etapa de revisão da decisão automatizada mostra-se incompatível com a adequada proteção dos direitos dos titulares de dados.

No contexto do Judiciário Federal brasileiro, Rossetti (2025) [26] identifica riscos específicos ao diferenciar “*decisões humanas amparadas por algoritmos*” — correspondentes aos Sistemas Automatizados de Suporte à Decisão (ADSS) — de “*decisões automatizadas que substituem as decisões humanas*” — correspondentes aos Sistemas de Decisão Totalmente Automatizada (FADS).

No primeiro cenário, o algoritmo atua estritamente como ferramenta de apoio, por exemplo, na busca rápida de jurisprudência ou na triagem inicial de processos. A essência desse modelo é que a decisão final e o poder de julgamento permanecem integralmente com o magistrado. O risco é considerado baixo ou controlado, pois o foco recai sobre o ganho de eficiência, mantendo-se o controle humano e a responsabilização institucional (*accountability*).

No segundo cenário, o sistema algorítmico passa a tomar a decisão final de forma automatizada, sem intervenção humana, configurando clara substituição da atividade judicante.

Segundo a autora, esse modelo gera riscos mais significativos, como a estagnação da jurisprudência e a dificuldade de explicação das razões decisórias, uma vez que o poder decisório é transferido da esfera humana para um sistema não humano.

Nessa transferência, destaca-se, primeiramente, o risco de estagnação da jurisprudência. Os algoritmos, por sua natureza, são programados para aprender e replicar padrões de decisões passadas, tendendo a perpetuar o status quo decisório. O impacto reside na redução da capacidade evolutiva e adaptativa do direito, inerente à atuação do Poder Judiciário.

Ao automatizar parcela relevante dos julgados, o sistema pode dificultar a inovação e a adaptação da jurisprudência a novas realidades sociais e jurídicas, resultando em decisões rígidas e, potencialmente, na manutenção de desigualdades estruturais.

Em segundo lugar, destaca-se o risco de dificuldade de explicação das razões decisórias. Esse problema remete ao fenômeno da “caixa-preta” (*black box*) dos sistemas de inteligência artificial mais complexos. Nesses casos, torna-se desafiador, ou até inviável, explicar de forma inteligível às partes processuais interessadas como o algoritmo chegou a determinada conclusão.

O impacto dessa opacidade é grave, pois, segundo a autora [26], a garantia da justiça material exige que os atos decisórios do Poder Judiciário sejam públicos e devidamente fundamentados, conforme estabelecem o art. 93, inciso IX, da Constituição Federal, e o art. 11 do Código de Processo Civil.

A ausência de fundamentação adequada pode acarretar a nulidade da decisão, além de comprometer o direito à transparência e à explicabilidade previsto na LGPD, especialmente em seu art. 20, fragilizando, em última instância, a confiança no sistema de justiça.

Por todo o exposto, a literatura sobre Tomada de Decisão Automatizada (ADM) indica que, ao viabilizar decisões mais rápidas, precisas e fundamentadas em grandes volumes de dados, os Sistemas de Decisão Automatizada (ADS) apresentam potencial para gerar benefícios relevantes no setor público, como o aumento da eficiência e a redução de custos operacionais, bem como contribui para a desburocratização de tarefas complexas, fortalecendo a capacidade decisória das instituições.

No entanto, os autores citados anteriormente convergem ao alertar para riscos significativos associados à adoção desses sistemas, como ameaças à privacidade, possibilidade de discriminação decorrente de vieses algorítmicos, impactos desproporcionais sobre determinados grupos e desafios relacionados à transparência e à governança, sobretudo quando a supervisão humana é reduzida ou inexistente.

Acrescenta-se, ainda, a preocupação com práticas fraudulentas, seja pela exploração de vulnerabilidades tecnológicas seja pela manipulação de dados e documentos que alimentam os sistemas, fatores que podem comprometer a integridade das decisões automatizadas.

Nesse último contexto, é interessante observar que a fraude aparece na literatura tanto como risco quanto como campo de aplicação da ADM. A detecção de fraudes é frequentemente

apontada como um dos principais usos desses sistemas, sobretudo em áreas como gestão tributária e benefícios sociais [22], [27], [28].

No campo tributário, tais sistemas são associados ao aumento da conformidade fiscal, à detecção de evasão, de operações suspeitas e fraudes [22], [28]. Já no âmbito dos benefícios sociais, a literatura registra o uso de sistemas automatizados para controle de elegibilidade, identificação de pagamentos indevidos e investigação de possíveis fraudes, embora ressalte que essas aplicações exigem salvaguardas robustas, em razão dos riscos de vieses discriminatórios, falsos positivos e impactos desproporcionais sobre grupos vulneráveis [24], [27].

Entretanto, a despeito desse potencial de uso da ADM para fins de detecção e prevenção de fraudes, a automação também pode viabilizar fraudes em larga escala ou, até mesmo, produzir decisões injustas, como acusações indevidas de fraude, especialmente quando há falhas de governança ou a utilização de critérios discriminatórios ou insuficientes, como evidenciado no caso da Austrália, Robodebt, analisado por Rinta-Kahila et al. [24].

Ainda no âmbito dos benefícios sociais, a fraude em sistemas automatizados, especialmente quando as decisões são totalmente automatizadas, representa uma gravidade ainda maior, pois pode gerar prejuízos econômico-sociais em larga escala, impactando diretamente populações vulneráveis, comprometendo sua subsistência e enfraquecendo a confiança nas instituições públicas [27].

Por tudo isso, alguns autores discutem a importância da revisão humana como salvaguarda essencial para mitigar riscos e garantir a legitimidade das decisões automatizadas. Modelos híbridos, nos quais humanos e algoritmos compartilham a tomada de decisão, são defendidos como uma alternativa para evitar vieses e erros sistêmicos.

Assim, embora a Tomada de Decisão Automatizada (ADM) represente avanços inegáveis, sua adoção deve estar, necessariamente, acompanhada de mecanismos de governança, transparência e supervisão humana, sobretudo no enfrentamento de fraudes e na proteção de direitos fundamentais.

III. METODOLOGIA

Este estudo caracteriza-se como pesquisa de natureza exploratória, pois pretende proporcionar melhor entendimento do problema, visando esclarecer conceitos, aprimorar ideias, construir hipóteses ou descobrir novas intuições [29]. Adota-se uma abordagem qualitativa, que não se restringe à quantificação, mas busca compreender e interpretar fenômenos do mundo real [30].

Para o melhor entendimento do problema e análise de seus impactos, a pesquisa documental envolveu o exame de legislações nacionais e estrangeiras (como LGPD, GDPR, AI Act, e outros), resoluções e guias interpretativos de autoridades (como ANPD, TCU, Comissão Europeia e OCDE), além de documentos públicos (relatórios técnicos, pareceres públicos, julgados e estudos de casos) relacionados à automação de decisões por órgãos públicos em áreas como saúde, segurança

pública, fiscalização tributária e benefícios previdência e sociais).

Ressalta-se que todos os dados utilizados são públicos, não havendo coleta direta de dados com participantes nem tratamento de informações pessoais, sensíveis ou sigilosas.

Além disso, ainda que o estudo não envolva desenvolvimento, teste ou exploração de sistemas reais, nem tratamento direto de dados pessoais, foram observados, como parâmetros de cautela, os princípios da Lei Geral de Proteção de Dados Pessoais, especialmente os princípios da finalidade, necessidade e transparência, previstos no art. 6º da LGPD [2].

Desse modo, a análise documental foi conduzida de forma a utilizar apenas informações necessárias ao objetivo do estudo, para assegurar rastreabilidade e transparência na interpretação dos documentos examinados.

IV. RESULTADOS E DISCUSSÃO

A análise dos dados obtidos por meio da revisão bibliográfica, da investigação documental e da avaliação crítica de experiências nacionais e internacionais permite identificar um conjunto consistente de resultados acerca das potencialidades e dos impactos das decisões automatizadas no reconhecimento de direitos por órgãos públicos brasileiros.

Esses resultados evidenciam que, não obstante as potencialidades da automação decisória como instrumento de modernização administrativa e de ampliação da capacidade operacional do Estado [3], [5], [27], sua implementação dissociada de salvaguardas normativas, técnicas e institucionais adequadas tem gerado preocupações relevantes, especialmente quando associada a técnicas de inteligência artificial [16], [18].

Tais preocupações manifestam-se, principalmente, na integridade do processo decisório, em razão dos riscos associados à opacidade algorítmica, à reprodução de vieses, à dificuldade de explicação das decisões e à limitação do controle social e institucional sobre os critérios empregados pelos sistemas automatizados [17], [21], [26].

Ademais, embora a inteligência artificial constitua importante ferramenta para automação de detecção de irregularidades e identificação de padrões suspeitos em grandes volumes de dados, sua utilização sem mecanismos adequados de supervisão, auditoria e validação humana pode comprometer a própria prevenção de fraudes, favorecendo a produção de falsos positivos, classificações inadequadas e decisões equivocadas com repercussões relevantes para os administrados [8], [22], [27].

Soma-se a isso o fato de que falhas na governança dos sistemas automatizados podem resultar em violações de direitos, especialmente quando inexistem transparência, possibilidade efetiva de contestação e revisão humana das decisões automatizadas [17], [21], [24].

A. Expansão da decisão automatizada no setor público e deslocamento do risco decisório

Os resultados indicam que a adoção de Sistemas de Decisão Automatizada (ADS), em especial aqueles configurados como Sistemas de Decisão Totalmente Automatizada (FADS), tem

ganhado força no setor público brasileiro na última década, sobretudo em áreas caracterizadas por alto volume processual, padronização de critérios e pressão por eficiência administrativa. Esse movimento é particularmente visível em políticas públicas de caráter massivo, como concessão e revisão de benefícios sociais e previdenciários.

Todavia, verifica-se que a automação decisória promove um deslocamento do risco decisório institucional. Tradicionalmente, falhas decisórias encontravam-se associadas a erros individuais de servidores ou agentes públicos, normalmente passíveis de correção por mecanismos de supervisão hierárquica, revisão administrativa ou controle recursal.

Com a adoção de sistemas automatizados, contudo, parte desse risco assume caráter sistêmico, pois eventuais inconsistências nos dados de entrada, erros de modelagem, critérios inadequados de classificação ou vieses incorporados aos algoritmos podem ser reproduzidos de forma automática e em larga escala, afetando simultaneamente um número expressivo de administrados [16], [18], [21].

A literatura também indica que esse fenômeno altera significativamente a relação entre eficiência e controle institucional. Enquanto erros humanos tendem a ocorrer de maneira pontual e dispersa, falhas em sistemas automatizados possuem potencial de escalabilidade, permitindo que uma única deficiência técnica se propague por milhares de decisões antes mesmo de ser identificada ou corrigida [18], [26]. Nesses casos, o impacto do erro deixa de ser apenas individual e passa a representar um risco institucional mais amplo.

Assim, a literatura sugere que decisões incorretas decorrentes de falhas técnicas, vieses algorítmicos, manipulação de dados ou fraudes associadas a sistemas automatizados deixam de constituir eventos isolados e passam a apresentar potencial de impacto coletivo, ampliando significativamente seus efeitos jurídicos, sociais e econômicos, uma vez que os mesmos critérios decisórios podem ser aplicados simultaneamente a um grande universo de casos, como observado no caso Robodebt [24].

Ademais, esse deslocamento do risco decisório para uma dimensão sistêmica pode dificultar a efetividade dos mecanismos tradicionais de responsabilização. Em situações envolvendo cadeias complexas de desenvolvimento, treinamento, parametrização, supervisão e operação dos sistemas automatizados, a identificação dos agentes efetivamente responsáveis por erros, fraudes, falhas de supervisão ou deficiências de governança tende a tornar-se mais complexa.

Como consequência, os custos decorrentes de decisões automatizadas equivocadas podem ser absorvidos pelo próprio Estado e, em última instância, socializados entre toda a coletividade, sem que haja correspondente individualização das responsabilidades ou recomposição integral do dano ao erário.

B. Limitações operacionais dos sistemas automatizados e fragilidade da decisão totalmente automatizada

Em geral, sistemas automatizados operam a partir de pressupostos formais e estatísticos. Por essa razão, nem sempre

incorporam de modo satisfatório elementos contextuais, exceções fáticas complexas e nuances socioeconômicas presentes nos casos concretos submetidos à administração pública.

Essa limitação torna-se especialmente relevante no âmbito das relações jurídicas subjetivas e evidencia uma das principais fragilidades operacionais desses sistemas.

Nos Sistemas de Decisão Totalmente Automatizada (FADS), a ausência de supervisão humana efetiva intensifica essa limitação. O algoritmo, ao aplicar regras ou modelos preditivos, tende a tratar situações formalmente semelhantes como equivalentes, ainda que materialmente distintas. Tal característica se mostra particularmente problemática no reconhecimento de direitos sociais e previdenciários, nos quais pequenas variações fáticas podem produzir consequências jurídicas substancialmente diferentes.

No âmbito do Instituto Nacional do Seguro Social (INSS), autarquia a que pertence este autor, por exemplo, essa limitação revela-se de forma especialmente sensível, uma vez que a análise de benefícios previdenciários e assistenciais frequentemente envolve elementos subjetivos, históricos contributivos complexos, vínculos laborais atípicos, períodos de informalidade e situações de vulnerabilidade social que não são plenamente captáveis por modelos automatizados.

A título exemplificativo, considere-se a análise automatizada de pedidos de benefícios assistenciais. Nessa hipótese, um sistema automatizado programado para aplicar estritamente o critério legal de renda familiar per capita indefere automaticamente requerimentos de grupos familiares cuja renda ultrapasse minimamente o limite estabelecido. Contudo, duas famílias com renda formal semelhante podem apresentar condições materiais profundamente distintas. Enquanto uma delas pode possuir moradia própria e não incorrer em gastos extraordinários, outra pode arcar com despesas contínuas de aluguel, medicamentos ou cuidados especiais relacionados à deficiência de um de seus membros. Embora essas circunstâncias sejam juridicamente relevantes para a compreensão da situação concreta de vulnerabilidade, sistemas totalmente automatizados tendem a classificá-las de forma idêntica.

A utilização exclusiva de decisões automatizadas no reconhecimento de direitos assistenciais e previdenciários tem evidenciado uma tendência estrutural à desconsideração de situações fáticas específicas e de exceções juridicamente relevantes. Como consequência, observa-se a produção de indeferimentos padronizados, baseados em regras de negócio rígidas e em dados incompletos constantes dos sistemas cadastrais de informações sociais utilizados como parâmetros de entrada dessas decisões.

Nesse contexto, o Relatório de Avaliação nº 1205147, de 09 de outubro de 2023, elaborado pela Controladoria-Geral da União (CGU) [31], indica que a ampliação da análise automática coincidiu com um crescimento significativo dos indeferimentos administrativos. Segundo o relatório, enquanto nas análises manuais houve uma leve redução do percentual de negativas, nas análises automáticas verificou-se aumento expressivo desse índice, sugerindo que parte das decisões anteriormente proferidas manualmente passou a ser processada

de forma automatizada [31].

O mesmo relatório também chama atenção para os efeitos decorrentes de indeferimentos potencialmente indevidos. Segundo a CGU, essas decisões tendem a ampliar a demanda por revisões administrativas, recursos e ações judiciais, contribuindo para o aumento da litigiosidade tanto na esfera administrativa quanto na judicial. Esse cenário revela que negativas automatizadas ou inadequadamente fundamentadas podem apresentar maior probabilidade de contestação pelos segurados [31].

Dessa forma, sistemas totalmente automatizados transferem, na prática, ao requerente o ônus de identificar falhas sistêmicas, interpor recursos administrativos ou recorrer ao Poder Judiciário para reverter decisões potencialmente indevida [31]. Tal dinâmica acaba por inverter a lógica protetiva que historicamente orienta o direito previdenciário brasileiro, deslocando para o segurado a responsabilidade de corrigir, *a posteriori*, falhas do próprio aparato decisório estatal.

C. Opacidade decisória, rastreabilidade limitada e fragilização do controle institucional

Para além das limitações operacionais já mencionadas, os resultados também evidenciam problemas relacionados à opacidade decisória, conhecida como efeito “caixa-preta”. A dificuldade central está no fato de que a falta de transparência não compromete apenas o exercício, pelo cidadão, do direito à explicação sobre decisões que lhe negam direitos. Ela também afeta a atuação dos órgãos de controle interno e externo, que passam a enfrentar barreiras técnicas relevantes para auditar os critérios decisórios adotados.

Essa dificuldade de acesso aos critérios efetivamente empregados nos processos decisórios, sobretudo quando mediados por sistemas digitais complexos, integrados às mais diversas bases de dados e sistemas legados, compromete a rastreabilidade das decisões administrativas e limita a verificação de sua conformidade jurídica e de sua aderência plena à finalidade pública a que se destina.

No que se refere à opacidade, o Tribunal de Contas da União (TCU) tem ressaltado a importância da transparência e da governança da informação no setor público. No Acórdão 2876/2025 – Plenário, o TCU apontou que a falta de clareza sobre os dados compromete o controle social, enfraquece a *accountability* e pode favorecer decisões insuficientemente fundamentadas, reforçando a necessidade de aprimoramento da governança informacional [32]. Mais ainda, em sentido semelhante, no Acórdão 1511/2025 – Plenário, a Corte destacou que a administração pública deve evitar a formação de zonas de opacidade, especialmente em contextos nos quais a transparência deve orientar a atuação estatal [33].

D. Insuficiência da supervisão humana no modelo jurídico brasileiro

Além disso, o modelo jurídico brasileiro de proteção do titular de direitos em decisões automatizadas apresenta limitações quando analisado à luz da experiência europeia inaugurada pelo Regulamento Geral de Proteção de Dados (GDPR) [34].

Embora o art. 20 da Lei Geral de Proteção de Dados (LGPD) reconheça o direito à revisão das decisões tomadas unicamente com base em tratamento automatizado, não explicita que essa revisão deva ser conduzida por agente humano dotado de efetivo poder decisório [35]. Em contraste, o GDPR estrutura a proteção do titular a partir da exigência de intervenção humana significativa, orientada à possibilidade real de contestação, reconsideração e modificação do resultado decisório, se for o caso.

Conforme determina o Artigo 22 do GDPR [34], o titular dos dados tem o direito de não ficar sujeito a decisões tomadas exclusivamente com base em tratamento automatizado, devendo o controlador dos dados adotar medidas adequadas para salvaguardar os direitos, liberdades e interesses legítimos do titular, incluindo, ao menos, o direito de obter intervenção humana, manifestar seu ponto de vista e contestar a decisão.

Essa exigência é normativamente fortalecida pelo Regulamento Europeu de Inteligência Artificial (AI Act) [36], que trata a supervisão humana (*human oversight*) como elemento estrutural da governança de sistemas algorítmicos de alto risco, categoria na qual se inserem os sistemas de decisões automatizadas capazes de produzir efeitos significativos sobre direitos fundamentais.

Tal enquadramento revela-se plenamente compatível com o entendimento adotado pela Autoridade Nacional de Proteção de Dados (ANPD), especialmente no âmbito da Resolução CD/ANPD nº 2/2022 [37], que reconhece a existência de operações de tratamento de dados pessoais aptas a ensejar riscos elevados aos titulares.

A Resolução CD/ANPD nº 2/2022 define como de alto risco as operações de tratamento de dados pessoais capazes de produzir impactos relevantes sobre interesses e direitos fundamentais dos titulares. Nesse conjunto, incluem-se as decisões baseadas exclusivamente em tratamento automatizado de dados pessoais, especialmente quando voltadas à definição de perfis relacionados à vida pessoal, profissional, à saúde, ao consumo, ao crédito ou a outros aspectos da personalidade do titular [37].

Nessa direção, o art. 14 do AI Act determina que os sistemas de inteligência artificial classificados como de alto risco sejam projetados de modo a permitir supervisão efetiva por pessoas naturais ao longo de todo o período de sua utilização. O próprio regulamento esclarece que essa supervisão tem por objetivo prevenir ou reduzir riscos à saúde, à segurança e aos direitos fundamentais. Com isso, reforça-se a exigência de controle humano qualificado nos casos em que decisões automatizadas possam produzir efeitos relevantes sobre a esfera jurídica dos indivíduos [36].

Para que a supervisão humana não se limite a uma exigência meramente formal, o AI Act estabelece que os responsáveis pelo acompanhamento do sistema devem dispor de condições reais para intervir de maneira qualificada. Isso pressupõe que compreendam as capacidades e limitações relevantes do sistema de IA de alto risco, acompanhem seu funcionamento e sejam capazes de identificar e responder a anomalias, falhas ou comportamentos inesperados durante sua operação [36].

Além disso, o AI Act atribui ao supervisor humano uma prerrogativa efetiva de intervenção, ao prever que ele possa optar por não utilizar o sistema ou interromper seu funcionamento quando necessário. Com isso, a supervisão deixa de ser apenas formal e passa a envolver poder concreto sobre a operação do sistema e sobre seus efeitos decisórios [36].

À luz desse modelo regulatório, evidencia-se que o art. 20 da LGPD permanece em um nível normativo significativamente inferior, ao permitir que revisões meramente formais — ou condicionadas aos mesmos parâmetros automatizados que orientaram a decisão originária — sejam apresentadas como cumprimento do dever legal, sem assegurar uma reavaliação humana substantiva, crítica e dotada de autoridade decisória efetiva.

Esse déficit normativo fragiliza a proteção material dos administrados e compromete a *accountability* estatal em contextos de decisão pública massificada e mediada por sistemas de decisões automáticas, especialmente quando tais sistemas são adotados como resposta gerencial à necessidade de reduzir filas de espera extensas e persistentes, convertendo a automação do processo decisório em instrumento prioritário de vazão de demanda, em detrimento da análise qualificada do mérito individual dos requerimentos.

E. Riscos de fraude

Ato contínuo, os resultados da pesquisa indicam que a automação decisória, ao mesmo tempo em que é frequentemente apresentada como instrumento de combate à fraude, cria novas superfícies de vulnerabilidade que podem ser exploradas por agentes mal-intencionados.

Diferentemente da fraude tradicional, baseada na interação direta entre indivíduos e agentes públicos, a fraude em ambientes automatizados tende a assumir caráter técnico, sistêmico e, muitas vezes, silencioso.

Entre os principais riscos identificados, destacam-se:

1) *A manipulação dos dados de entrada que alimentam os sistemas automatizados*: risco que se materializou de forma emblemática no caso da denominada “Operação Sem Desconto”, que revelou a existência de um esquema fraudulento de grandes proporções envolvendo o cadastro e a manutenção indevida de descontos associativos em benefícios previdenciários do INSS.

Nesse contexto, a inserção e a validação automática de informações falsas ou indevidamente autorizadas nos sistemas corporativos permitiram que dados contaminados fossem tratados como legítimos pelo processo decisório automatizado de descontos associativos, viabilizando a continuidade de descontos irregulares sem detecção imediata.

O caso evidencia que, uma vez comprometida a camada de entrada dos dados — seja por falhas de controle ou exploração de vulnerabilidades procedimentais — o sistema automatizado tende a reproduzir o erro de forma sistêmica e persistente, conferindo aparência de legalidade a decisões materialmente viciadas e ampliando exponencialmente o impacto financeiro e social da fraude;

2) *A exploração de regras decisórias rígidas e previsíveis*: característica inerente a sistemas de decisão automatizada, cuja lógica opera a partir de parâmetros fixos, fluxos determinísticos e critérios previamente codificados. Essa rigidez decisória cria incentivos claros para a adaptação estratégica de comportamentos fraudulentos, uma vez que agentes maliciosos passam a conhecer — ou a inferir — os requisitos formais mínimos necessários para a validação automática de determinados atos, como autorizações, vínculos ou elegibilidades.

A previsibilidade das regras algorítmicas desses sistemas permite, assim, que fraudes sejam estruturadas para “passar pelo sistema”, atendendo artificialmente aos critérios exigidos, ainda que desprovidas de substância jurídica ou fática.

Diferentemente da análise humana, que tende a identificar incoerências contextuais, padrões atípicos ou indícios de irregularidade não formalizáveis, o sistema automatizado reproduz decisões de forma acrítica sempre que os parâmetros de entrada aparentam conformidade, transformando a rigidez normativa em vetor de vulnerabilidade institucional.

Esse cenário favorece a consolidação de fraudes repetitivas e escaláveis, com elevado impacto financeiro e dificuldade de detecção tempestiva, sobretudo quando inexistem mecanismos de supervisão humana significativa; e

3) *O comprometimento da infraestrutura tecnológica subjacente, seja por ataques externos, seja por ações internas maliciosas*: risco que se manifesta quando os sistemas que sustentam a decisão automatizada têm sua integridade, disponibilidade ou confiabilidade violadas. Em ambientes altamente digitalizados, como os utilizados por alguns órgãos públicos federais, a exemplo do INSS, a infraestrutura tecnológica deixa de ser mero suporte operacional e passa a integrar o próprio núcleo da função decisória.

Assim, a inserção de dados falsos em bases de dados, a modificação indevida de parâmetros sistêmicos ou o acesso não autorizado a módulos críticos pode resultar na emissão de decisões automatizadas materialmente ilegítimas, ainda que formalmente válidas sob a lógica interna do sistema.

Esses riscos guardam semelhança com aqueles observados no Poder Judiciário brasileiro em decorrência de ataques hackers, nos quais a violação de sistemas informatizados afetou não apenas a disponibilidade dos serviços, mas, sobretudo, a integridade do próprio processo decisório.

Conforme documentado por Alves, Georg e Nunes (2022), em ataques cibernéticos recentes “foram levantadas evidências de que um hacker obteve acesso ao sistema processual eletrônico, possibilitando a mudança de pareceres do MPU, a conversão de sentenças de condenação em absolvição e a alteração das contas destinatárias para o recebimento de valores legítimos em outros processos”, demonstrando que a invasão de infraestruturas digitais críticas pode produzir decisões formalmente válidas, porém materialmente viciadas [38].

Os autores também destacam que esses episódios expõem fragilidades que vão além da interrupção temporária de serviços, pois podem afetar a integridade dos dados e comprometer a confiança nas instituições. Esse cenário reforça a necessidade

de mecanismos mais robustos de governança e de segurança da informação [38].

Essa dinâmica evidencia que, tanto no âmbito judicial quanto no administrativo, a manipulação indevida de sistemas digitais pode afetar diretamente direitos e obrigações dos cidadãos, reforçando a importância da integridade informacional como condição de legitimidade material das decisões automatizadas.

No contexto da decisão administrativa automatizada, especialmente em políticas públicas de massa, falhas na infraestrutura tecnológica podem produzir danos em escala ampliada. Uma única vulnerabilidade de segurança ou um ato malicioso pode afetar simultaneamente milhares de decisões e vidas.

Com isso, fragiliza-se a confiança institucional, aumenta-se o risco de fraudes sistêmicas e evidencia-se a necessidade de integrar governança e segurança cibernética no setor público.

F. Diretrizes emergentes de governança para mitigação de riscos

À luz dos resultados apresentados, a mitigação dos riscos associados às decisões automatizadas por órgãos públicos não demanda a rejeição da automação decisória, cuja adoção se consolidou como elemento estrutural da atuação estatal contemporânea, mas a reconfiguração de seus arranjos de governança, de modo a compatibilizar eficiência operacional, proteção de direitos e *accountability*. Nesse sentido, emergem as seguintes diretrizes:

1) *Institucionalização da Supervisão Humana Significativa (human oversight)*: diferentemente da revisão passiva, a governança deve assegurar que agentes públicos capacitados tenham autoridade técnica e jurídica para intervir no ciclo de vida do processo decisório. Essa diretriz pode ser viabilizada por meio de:

- reserva de cotas de amostragem para análise humana obrigatória, sobretudo em decisões classificadas de alto risco, para aferição de conformidade contextual; e
- pedido de revisão significativo, processado por um fluxo apartado, em que o agente revisor tenha autonomia para reformar o mérito e não apenas validar a consistência lógica do algoritmo da decisão automatizada.

2) *Implementação de Auditorias Algorítmicas e Testes de Integridade*: os órgãos devem realizar auditorias periódicas e, sempre que possível, independentes para detectar vieses sistêmicos e vulnerabilidades a fraudes. Essa diretriz pode ser viabilizada por meio de:

- testes de intrusão (pentest) com simulação de ataques e tentativas de inserção de dados espúrios para avaliar a robustez dos sistemas e identificar vulnerabilidades, falhas de configuração e brechas de segurança que possam ser exploradas por agentes mal-intencionados. No Brasil, os órgãos podem ser auxiliados pelo Centro Integrado de Segurança Cibernética do Governo Digital (CISC Gov.br); e
- análise estatística de desvios nos padrões das decisões (como observado no salto de 41% para 65% de inde-

ferimentos identificado pela CGU), disparando alertas automáticos de necessidade de supervisão humana.

3) *Fortalecimento da Transparência e do Direito à Explicação*: a opacidade decisória do “efeito caixa-preta” deve ser combatida por meio de camadas de explicabilidade com notas explicativas da lógica decisória. Essa diretriz pode ser viabilizada por meio de:

- árvore de decisão, em linguagem natural, e memória de cálculo de todo ato administrativo automatizado, permitindo que o cidadão compreenda quais fatos ou dados foram determinantes para a negativa ou reconhecimento de seu direito.
- sistema de registro (logs) das informações utilizadas na tomada de decisão, facilitando, dentre outros, a identificação de onde ocorreu a corrupção do dado em caso de erro ou fraude.

4) *Governança de Dados de Entrada e Saneamento de Bases Legadas*: a propensão da automação em replicar e amplificar erros originados de bases de dados viciadas deve ser mitigada mediante a estruturação de fluxos contínuos de higienização de dados. Essa diretriz pode ser viabilizada por meio de:

- protocolos de validação cruzada, em que o sistema não deve decidir com base em uma única fonte de dados se houver divergência entre as bases governamentais “integradas”, por exemplo, divergência entre as bases da Receita Federal e do INSS deve gerar “pendência de supervisão humana” automática; e
- mecanismos de autodeclaração retificadora, para permitir que o usuário, no momento do requerimento, aponte inconsistências em seus dados cadastrais antes do processamento da decisão, evitando o indeferimento evitável.

5) *Gestão de Responsabilidade e Accountability*: o deslocamento do risco decisório para o cidadão e a consequente socialização dos prejuízos decorrentes de falhas no processo decisório automatizado devem ser combatidos mediante a clara delimitação de responsabilidades institucionais e funcionais. Essa diretriz pode ser viabilizada por meio de:

- matriz de responsabilização do sistema, com definição clara, em normativos internos, dos responsáveis pela homologação do código-fonte, pela curadoria dos dados, pela supervisão operacional (dos dados de entrada) e pela supervisão das decisões (dados de saída); e
- protocolos de remediação e fluxos de reparação (*playbooks* e *runbooks*): estabelecendo roteiros procedimentais pré-definidos para resposta a incidentes envolvendo sistemas automatizados. Como, por exemplo, a criação de playbooks de resposta a incidentes (manuais de procedimentos para interrupção imediata do sistema em caso de detecção de anomalias estatísticas ou erros em cascata, garantindo a continuidade do serviço público por vias manuais enquanto o sistema é auditado); e implementação de runbooks de reparação *ex-officio* (fluxos automatizados de reversão de decisões ao identificarem um erro sistêmico na lógica decisória ou na base de dados,

disparando automaticamente o reprocessamento de todos os atos administrativos afetados, independentemente de provocação do cidadão, em observância ao princípio da autotutela administrativa).

Por fim, para facilitar a compreensão e a aplicação prática das recomendações por gestores e decisores públicos, segue a Tabela I com as diretrizes de governança propostas para decisões automatizadas no setor público.

Tabela I
DIRETRIZES DE GOVERNANÇA PARA DECISÕES AUTOMATIZADAS NO SETOR PÚBLICO. FONTE: AUTORAL.

Diretriz	Descrição resumida	Exemplos de aplicação/prática
Supervisão humana significativa	Garantir intervenção efetiva de agentes públicos capacitados no ciclo decisório, com autonomia real.	Amostragem obrigatória; revisão autônoma.
Auditorias algorítmicas e testes de integridade	Realizar auditorias periódicas e independentes para detectar vieses e vulnerabilidades.	Pentests; análise estatística de desvios.
Transparência e direito à explicação	Combater a opacidade decisória por meio de explicabilidade e registro dos critérios utilizados.	Árvore de decisão; logs detalhados.
Governança de dados de entrada	Validar e sanear bases de dados, evitando decisões baseadas em informações viciadas.	Validação cruzada; autodeclaração retificadora.
Gestão de responsabilidade e accountability	Definir matriz de responsabilização e protocolos de resposta a incidentes.	Playbooks; runbooks de reparação <i>ex officio</i> .

V. CONCLUSÃO

O presente estudo analisou as potencialidades e os impactos das decisões automatizadas no reconhecimento de direitos no âmbito da administração pública brasileira, com ênfase nas limitações operacionais, nos riscos de fraude e nos desafios relacionados à governança desses sistemas.

A partir de revisão bibliográfica crítica, análise documental e exame de casos paradigmáticos nacionais e internacionais, evidenciou-se que a adoção de sistemas de decisão automatizada constitui fenômeno irreversível e estrutural da transformação digital do setor público, capaz de gerar ganhos expressivos de eficiência, escala e padronização.

Todavia, demonstrou-se que tais benefícios precisam estar acompanhados de salvaguardas institucionais adequadas. Na ausência dessas garantias, a automação decisória tende a produzir efeitos adversos relevantes, como o aumento de indeferimentos indevidos, a ampliação da litigiosidade administrativa e judicial, a fragilização da transparência e a potencial violação de direitos fundamentais, especialmente em políticas públicas de caráter massivo.

Nesse sentido, os resultados indicam que a expansão dos sistemas de decisão automatizada, especialmente daqueles configurados como sistemas totalmente automatizados, promove um deslocamento significativo do risco decisório, que deixa de ser predominantemente individual (erro humano pontual)

para assumir natureza sistêmica, com efeitos potencialmente massificados.

Verificou-se, ainda, que tais sistemas apresentam limitações operacionais relevantes, particularmente na incapacidade de captar nuances fáticas, contextuais e socioeconômicas, o que se revela crítico em áreas como o reconhecimento de direitos previdenciários e assistenciais. Esse cenário conduz à produção de decisões padronizadas que, embora formalmente consistentes, podem ser materialmente inadequadas ou injustas.

Do ponto de vista institucional, a pesquisa evidenciou que a opacidade decisória, associada ao efeito “caixa-preta”, compromete a rastreabilidade das decisões e dificulta tanto o exercício do direito à explicação pelo cidadão quanto a atuação dos órgãos de controle. Somado a isso, o modelo jurídico brasileiro ainda apresenta lacunas relevantes, sobretudo pela ausência de previsão explícita de supervisão humana significativa na revisão de decisões automatizadas.

Adicionalmente, constatou-se que a automação, ao mesmo tempo em que é utilizada como ferramenta de combate à fraude, cria novas superfícies de vulnerabilidade, permitindo a ocorrência de fraudes técnicas, sistêmicas e escaláveis, seja por manipulação de dados de entrada, exploração de regras previsíveis, seja por comprometimento da infraestrutura tecnológica.

Diante desse cenário, a discussão crítica aponta que a simples adoção de tecnologias automatizadas não garante melhoria na prestação estatal de serviços de qualidade. Pelo contrário, quando dissociada de uma governança robusta, a automação pode intensificar desigualdades, transferir ônus indevidos ao cidadão e fragilizar legitimidade das decisões públicas.

À vista disso, o presente estudo buscou contribuir para o aprofundamento do debate sobre a tomada de decisão automatizada no setor público, ao evidenciar seus impactos concretos sobre o reconhecimento de direitos e sobre a dinâmica de riscos institucionais. Ao articular dimensões jurídicas, operacionais e tecnológicas, a pesquisa permite identificar não apenas os benefícios associados à automação, mas, sobretudo, seus limites estruturais e efeitos adversos, especialmente em contextos de decisão massificada.

As limitações deste estudo fornecem importantes diretrizes para o aprofundamento futuro das investigações sobre decisões automatizadas no setor público. Em primeiro lugar, destaca-se que a pesquisa possui natureza predominantemente qualitativa, baseada em revisão bibliográfica e análise documental, o que implica a possibilidade de interpretações condicionadas aos referenciais teóricos adotados.

Além disso, no que se refere à generalização dos resultados, ressalta-se que o estudo se concentrou no contexto da administração pública brasileira, com ênfase em experiências de conhecimento público que envolveram automação decisória em políticas públicas de grande escala. Dessa forma, os achados podem não ser integralmente aplicáveis a outros contextos institucionais com diferentes arranjos regulatórios, tecnológicos e organizacionais.

Ademais, reconhece-se que as diretrizes de governança propostas, embora estruturadas a partir da literatura e das evidências analisadas, podem enfrentar desafios práticos de implementação, tais como complexidade técnica, integração com sistemas legados, custos institucionais e necessidade de capacitação organizacional. Essas limitações, longe de invalidar os resultados, indicam caminhos concretos para pesquisas futuras e para o aprimoramento progressivo das práticas de automação no setor público.

Nessa perspectiva, destaca-se, inicialmente, a necessidade de desenvolver estudos empíricos de natureza quantitativa. Esses estudos poderiam mensurar, com maior precisão, os efeitos da automação sobre variáveis relevantes, como as taxas de reconhecimento e de indeferimento de direitos.

Também seria importante examinar os fenômenos de deslocamento de demanda. Esse deslocamento pode ocorrer tanto da esfera administrativa para a judicial quanto entre diferentes fases internas do processo administrativo. É o caso, por exemplo, de indeferimentos ou deferimentos incorretos que acabam dando origem a revisões e recursos.

Essas dinâmicas tendem a gerar retrabalho administrativo e sobrecarga institucional. Por isso, reforça-se a importância de produzir evidências mais robustas e sistematizadas sobre os impactos efetivos da decisão automatizada.

Mais ainda, futuras investigações podem explorar abordagens comparativas que envolvam diferentes órgãos, setores e configurações institucionais, com o objetivo de avaliar a capacidade de generalização dos achados — inclusive por meio da proposição de frameworks analíticos — e de identificar práticas bem-sucedidas passíveis de replicação em distintos contextos administrativos. Esse movimento é particularmente relevante diante da heterogeneidade dos modelos de automação adotados no âmbito da administração pública.

Em síntese, as perspectivas futuras indicam que o avanço da automação no setor público demandará não apenas evolução tecnológica, mas, sobretudo, o contínuo amadurecimento de modelos institucionais capazes de integrar eficiência, controle e proteção de direitos de forma equilibrada e sustentável.

REFERÊNCIAS

- [1] Brasil, “Lei n. 14.129, de 29 de março de 2021: dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública,” Diário Oficial da União, 2021, texto compilado. [Online]. Available: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/14129.htm
- [2] —, “Lei n. 13.709, de 14 de agosto de 2018: Lei Geral de Proteção de Dados Pessoais (LGPD),” Diário Oficial da União, 2018, texto compilado. [Online]. Available: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/13709.htm
- [3] M. M. Ribeiro and C. I. Segatto, “Inteligência artificial nas organizações públicas brasileiras: heterogeneidades e capacidades em tecnologia da informação,” *Revista de Administração Pública*, vol. 59, no. 1, pp. 1–20, 2025, e2024-0066.
- [4] Instituto Nacional do Seguro Social, “Automação é aliada na agilização das decisões do INSS,” Portal Gov.br, 2023, publicado em 19 jun. 2023 e atualizado em 16 jan. 2025. [Online]. Available: <https://www.gov.br/inss/pt-br/noticias/noticias/automacao-e-aliada-na-agilizacao-das-decisoes-do-inss>

- [5] S. C. Carvalho, "Transformação digital da Administração Pública e decisões automatizadas: o caso do INSS," Dissertação de mestrado, Fundação Getúlio Vargas, Escola Brasileira de Administração Pública e de Empresas, Rio de Janeiro, 2023, 83 f.
- [6] R. M. d. Oliveira, "Automação, IA e o impacto na eficiência do INSS," Dissertação de mestrado, Fundação Getúlio Vargas, Escola Brasileira de Administração Pública e de Empresas, Rio de Janeiro, 2024, 62 f.
- [7] B. d. S. Rocha and D. d. Oliveira, "Inteligência Artificial e Previdência Social: uma análise sobre o processo de automatização da concessão de benefícios previdenciários," *UNISANTA Law and Social Science*, vol. 14, no. 2, pp. 132–151, 2025.
- [8] A. P. V. C. Menezes, "Inteligência artificial para identificação de indícios de fraude e corrupção em compras públicas no TCU," Dissertação de mestrado, Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, Brasília, DF, 2021, 109 p. Orientador: Caio Cordeiro de Resende.
- [9] Conselho Nacional de Justiça, "Resolução n. 332, de 21 de agosto de 2020," Conselho Nacional de Justiça, 2020, dispõe sobre a ética, a transparência e a governança na produção e no uso de inteligência artificial no Poder Judiciário. [Online]. Available: <https://atos.cnj.jus.br/files/original191707202008255f4563b35f8e8.pdf>
- [10] —, "Programa Justiça 4.0: levantamento de projetos de inteligência artificial no Poder Judiciário," Conselho Nacional de Justiça, Brasília, DF, Tech. Rep., 2024, levantamento identificou projetos de inteligência artificial desenvolvidos ou em desenvolvimento em tribunais e conselhos de justiça em 2023.
- [11] V. C. L. L. Valle, J. R. Fuentes i Gasó, and A. M. Ajus, "Decisão judicial assistida por inteligência artificial e o Sistema Victor do Supremo Tribunal Federal," *Revista de Investigações Constitucionais*, vol. 10, no. 2, pp. 1–38, 2023, e252.
- [12] Tribunal de Contas da União, "Utilização de inteligência artificial na Administração Pública Federal," Tribunal de Contas da União, Brasília, DF, Tech. Rep., 2022, levantamento sobre o uso de inteligência artificial na Administração Pública Federal. [Online]. Available: <https://portal.tcu.gov.br/data/files/D0/C3/BC/DA/EF17781046756058F18818A8/Utilizacao%20de%20Inteligencia%20Artificial%20na%20Admistracao%20Publica.pdf>
- [13] A. A. J. Anastasia, "A Inteligência Artificial no controle de políticas públicas," *Revista do Tribunal de Contas do Estado de Minas Gerais*, no. Edição especial, pp. 42–50, 2024.
- [14] E. S. Vasconcelos and F. A. d. Santos, "Inteligência artificial na gestão pública brasileira: desafios e oportunidades para a eficiência governamental," *Revista Observatorio de la Economía Latinoamericana*, vol. 22, no. 6, pp. 1–21, 2024.
- [15] B. Lietz, "O uso da inteligência artificial e a fiscalização dos contribuintes na perspectiva dos direitos e deveres da relação tributária," Dissertação de mestrado, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2021, 137 f.
- [16] T. Sever, "Automated Decision-Making in Public Sector," in *The Future of Public Administration Enabled through Emerging Technologies: 31st NISPAcee Annual Conference*, 2023, pp. 1–13.
- [17] T. S. Barbosa, D. W. Toniazzo, and R. L. Ruaro, "O direito à explicação nas decisões automatizadas: uma abordagem comparativa entre o ordenamento brasileiro e europeu," *Revista Internacional CONSINTER de Direito*, pp. 55–69, 2021.
- [18] A. Rizk and I. Lindgren, "Automated Decision-Making in the Public Sector: A Multidisciplinary Literature Review," in *International Conference on Electronic Government*, ser. Lecture Notes in Computer Science, vol. 14841. Springer, 2024, pp. 237–253.
- [19] R. T. Sutton, D. Pincock, D. C. Baumgart, D. C. Sadowski, R. N. Fedorak, and K. I. Kroeker, "An overview of clinical decision support systems: benefits, risks, and strategies for success," *NPJ digital medicine*, vol. 3, no. 1, p. 17, 2020.
- [20] N. d. A. d. A. Sobrenome, "Título do Artigo Aqui," in *Direito, Governança e Novas Tecnologias II*. Florianópolis: CONPEDI, 2025.
- [21] C. Castelluccia and D. Le Métayer, *Understanding algorithmic decision-making: Opportunities and challenges*. European Parliament, 2019.
- [22] S. Rahman, M. Sirazy, R. Das, and R. Khan, "An exploration of artificial intelligence techniques for optimizing tax compliance, fraud detection, and revenue collection in modern tax administrations," *International Journal of Business Intelligence and Big Data Analytics*, vol. 7, no. 3, pp. 56–80, 2024.
- [23] Brasil. Receita Federal, "Malha Fiscal Digital (MFD)," Portal Gov.br, 2024, publicado em 28 maio 2015; atualizado em 24 jun. 2024. [Online]. Available: <https://www.gov.br/receitaefederal/pt-br/assuntos/orientacao-tributaria/declaracoes-e-demonstrativos/revisao-de-declaracao-o-malha/malha-fiscal-digital>
- [24] T. Rinta-Kahila, I. Someh, N. Gillespie, M. Indulska, and S. Gregor, "Managing unintended consequences of algorithmic decision-making: The case of robodebt," *Journal of Information Technology Teaching Cases*, vol. 14, no. 1, pp. 165–171, 2024.
- [25] R. Morton, *Mean Streak: A moral vacuum, a dodgy debt generator and a multi-billion-dollar government shake down-the powerful story of robodebt*, WINNER of the Walkley Book Award 2025. HarperCollins Australia, 2024.
- [26] R. Rossetti, "Riscos do uso de algoritmos de Inteligência Artificial no processo de tomada de decisão judicial," *Revista da Faculdade de Direito da UERJ*, no. 44, pp. e91016, 1–21, 2025.
- [27] OECD, "Ai and the future of social protection in oecd countries," OECD Publishing, Paris, Tech. Rep. 42, 2025. [Online]. Available: <https://doi.org/10.1787/7b245f7e-en>
- [28] —, "Ai in tax administration," Organisation for Economic Co-operation and Development, Paris, Tech. Rep., 2025, section of the report Governing with Artificial Intelligence. [Online]. Available: https://www.oecd.org/en/publications/governing-with-artificial-intelligence_nce_795de142-en/full-report/ai-in-tax-administration_30724e43.html
- [29] A. C. Gil, *Métodos e técnicas de pesquisa social*. 6. ed. Editora Atlas SA, 2008.
- [30] E. L. Da Silva and E. M. Menezes, "Metodologia da pesquisa e elaboração de dissertação," *UFSC, Florianópolis, 4a. edição*, vol. 123, no. 4, p. 138, 2005.
- [31] Controladoria-Geral da União, "Relatório de Avaliação: Instituto Nacional do Seguro Social – exercícios 2021 a 2023," Controladoria-Geral da União, Brasília, DF, Relatório de Avaliação 1205147, 2023, unidade auditada: Instituto Nacional do Seguro Social (INSS). [Online]. Available: <https://eaud.cgu.gov.br/relatorios>
- [32] Tribunal de Contas da União, "Acórdão n. 2876/2025 - TCU - Plenário," Tribunal de Contas da União, Plenário, 2025, processo TC 008.848/2024-6. Relator: Ministro Augusto Nardes. Código eletrônico: AC-2876-49/25-P. Publicado no BTCU Deliberações n. 229, de 10 dez. 2025. [Online]. Available: <https://pesquisa.apps.tcu.gov.br/redireciona/acordao-completo/ACORDAO-COMPLETO-2732212>
- [33] —, "Acórdão n. 1511/2025 - TCU - Plenário," Tribunal de Contas da União, Plenário, 2025, processo TC 023.096/2024-1. Relator: Ministro Antonio Anastasia. Código eletrônico: AC-1511-26/25-P. Representação relacionada ao Transferegov.br, LGPD e LAI. Publicado no BTCU Deliberações dos Colegiados do TCU e dos Relatores, ano 8, n. 129, de 18 jul. 2025. [Online]. Available: <https://pesquisa.apps.tcu.gov.br/redireciona/acordao-completo/ACORDAO-COMPLETO-2716769>
- [34] União Europeia, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation - GDPR)," Official Journal of the European Union, 2016, texto consolidado. [Online]. Available: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- [35] Brasil, "Lei n. 13.709, de 14 de agosto de 2018: Lei Geral de Proteção de Dados Pessoais (LGPD), art. 20," Diário Oficial da União, 2018, texto compilado. Art. 20 com redação dada pela Lei n. 13.853, de 8 de julho de 2019. [Online]. Available: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm
- [36] União Europeia, "Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento da Inteligência Artificial)," Jornal Oficial da União Europeia, 2024, link direto: <https://artificialintelligenceact.eu/article/14/>. [Online]. Available: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>
- [37] Autoridade Nacional de Proteção de Dados, "Resolução CD/ANPD n. 2, de 27 de janeiro de 2022," Diário Oficial da União, 2022, aprova o Regulamento de aplicação da Lei n. 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte. Publicada no Diário Oficial da União, Brasília, 28 jan. 2022, Seção 1, p. 6. [Online]. Available: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no-2-de-27-de-jan-eiro-de-2022
- [38] R. S. Alves, M. A. C. Georg, and R. R. Nunes, "Judiciário sob ataque hacker: riscos de negócio para segurança cibernética em tribunais brasileiros," *Revista Ibérica de Sistemas e Tecnologias de Informação*, no. E56, pp. 344–357, 2023.