ENAJUS Encontro de Administração da Justiça
João Pessoa
25 a 28 nov 2025

Controle de Armas de Fogo: Uma Análise da Atuação da Polícia Federal sob a Perspectiva da Governança Digital

Lucilene da Ressurreição Santos, Universidade de Brasília, Polícia Federal
Governança em Sistemas de Justiça

Resumo
O controle de armas de fogo no Brasil, instrumento vital para a segurança pública, é uma atribuição estratégica da Polícia Federal (PF), cuja atuação foi profundamente transformada pela digitalização dos processos. Com a explosão no número de Colecionadores, Atiradores e Caçadores (CACs), impulsionada por mudanças normativas, a PF tem utilizado sistemas informatizados para gerir essa demanda exponencial. Sob a perspectiva da governança digital, que preconiza o uso de Tecnologias da Informação e Comunicação (TICs) para aprimorar a eficiência administrativa e fortalecer valores democráticos como transparência e *accountability*, este artigo analisa os desafios e oportunidades dessa digitalização. A pesquisa adota uma abordagem qualitativa e exploratória, baseada em análise documental e normativa e na observação institucional aplicada, que permitiu identificar limitações práticas e gargalos operacionais dos sistemas no cotidiano das unidades da PF. O referencial teórico incluiu conceitos de governança eletrônica e, principalmente, de justiça algorítmica, que descreve decisões automatizadas sem clareza sobre como são formuladas. Os resultados indicam que, embora a informatização tenha trazido ganhos significativos como padronização de rotinas e agilidade na análise, ela impõe novos desafios. As principais deficiências incluem a opacidade dos critérios decisórios, instabilidade e lentidão dos sistemas, e a limitada integração com bases de dados externas essenciais. Acarreta ainda a dependência excessiva dos sistemas, carência de capacitação técnica dos servidores e o risco de exclusão digital. Conclui-se que, para que a digitalização se concretize com equidade e eficácia, é indispensável investir em segurança da informação, governança de dados, supervisão humana qualificada e revisão crítica dos sistemas. O trabalho visa subsidiar o aperfeiçoamento de políticas públicas para promover maior efetividade no controle de armas, sem comprometer direitos fundamentais.
Palavras-chave: Controle de Armas de Fogo; Polícia Federal; Governança Eletrônica; Justiça Algorítmica; Proteção de Dados; CACs.

1. Introdução

O controle de armas de fogo no Brasil figura como uma das atribuições mais sensíveis da administração pública, especialmente em um cenário de crescente preocupação com a segurança pública e o aumento da circulação de armamentos. A Polícia Federal (PF) exerce um papel central nesse processo, sendo a instituição responsável pelo registro,

controle, fiscalização e análise de pedidos de posse e porte de arma de fogo em âmbito nacional, conforme previsto no Estatuto do Desarmamento (Lei nº 10.826/2003) e regulamentações posteriores (Santos, 2025).

Nos últimos anos, o país assistiu a uma explosão no número de Colecionadores, Atiradores e Caçadores (CACs), impulsionada por mudanças normativas, flexibilizações e incentivos políticos. Segundo dados do Anuário Brasileiro de Segurança Pública (Fórum Brasileiro de Segurança Pública, 2023), o número de registros ativos de CACs ultrapassou a marca de 1 milhão em 2022, representando um aumento exponencial em relação aos anos anteriores. Esse crescimento impactou diretamente a estrutura e os sistemas da Polícia Federal, que precisaram absorver uma demanda crescente, sem que houvesse, necessariamente, o reforço correspondente em recursos humanos e tecnológicos.

Na prática, esse cenário tem gerado situações problemáticas. Em uma unidade, um requerente teve seu pedido de porte de arma indeferido automaticamente pelo sistema, sem justificativa clara ou possibilidade de recurso, ainda que tivesse apresentado toda a documentação exigida. Em outro caso, uma autorização foi concedida a um cidadão com histórico de violência doméstica não detectado pelo sistema, devido à ausência de integração com as bases judiciais estaduais. Esses exemplos ilustram como a informatização, se não for acompanhada de mecanismos de supervisão, explicabilidade e integração, pode comprometer a segurança pública e os direitos individuais.

A digitalização dos processos administrativos — especialmente por meio dos sistemas de controle de armas (SINARM, SINARM CAC e REGULA CAC) — buscou oferecer uma resposta moderna a essa nova realidade (Rodrigues & Cammarosano, 2022). Esses sistemas representam uma tentativa de modernização da gestão pública, permitindo maior agilidade nas análises, padronização de procedimentos e rastreabilidade das decisões. Trata-se de uma expressão da chamada governança digital, entendida como o uso estratégico de tecnologias da informação e comunicação (TICs) para melhorar a administração pública, promover a transparência e fortalecer valores democráticos como a *accountability* (Fabriz, Gomes & Mello, 2018; Guimarães & Medeiros, 2005).

Contudo, a promessa de eficiência da tecnologia esbarra em obstáculos conceituais e teóricos que merecem ser aprofundados. Embora os ganhos da informatização sejam evidentes, a prática nas unidades da Polícia Federal revela diversas limitações e desafios. As equipes responsáveis enfrentam sistemas instáveis, com falhas recorrentes, dificuldades de integração com bases externas (como o Judiciário e o Ministério Público), ausência de critérios decisórios públicos e compreensíveis nos sistemas automatizados, além da sobrecarga de trabalho provocada pela alta demanda (Santos, 2025). Em muitos casos, a promessa de eficiência da tecnologia esbarra em obstáculos operacionais e normativos que comprometem a efetividade e a justiça dos processos decisórios (Nascimento et al, 2025).

Com a edição do Decreto nº 11.615/2023, a Polícia Federal assumiu parte das atribuições antes exclusivas do Exército Brasileiro no controle de Colecionadores,

Atiradores e Caçadores (CACs). Essa transição implicou não apenas a gestão administrativa dessa categoria, mas também a incorporação de dados oriundos do SIGMA, sistema antes utilizado pelo Exército, em plataformas desenvolvidas pela PF (SINARM-CAC e REGULA-CAC). O processo revelou inúmeras fragilidades: inconsistências cadastrais, registros duplicados, serviços temporariamente indisponíveis e erros sistêmicos que afetam a análise dos pedidos. Além disso, a ausência de integração plena entre SIGMA e SINARM, somada às dúvidas jurídicas sobre a aplicação da nova legislação, gerou insegurança tanto para usuários quanto para servidores, evidenciando que a digitalização, sem governança digital robusta, pode replicar e até ampliar antigos gargalos burocráticos.

Este ensaio propõe-se a analisar os principais desafios teóricos que a digitalização dos processos de controle de armas na Polícia Federal enfrenta sob a perspectiva da governança digital. O problema central a ser explorado é: **quais são os principais desafios enfrentados pela Polícia Federal no uso dos sistemas informatizados de controle de armas (SINARM, SINARM-CAC e REGULA-CAC), diante do crescimento acelerado da demanda por parte dos CACs, e como a perspectiva da governança digital pode orientar soluções para melhorar a eficiência, a transparência e a segurança desses processos?**

O objetivo do presente artigo é lançar luz sobre esse dilema, propondo uma análise crítica e propositiva que articule a experiência prática das unidades com os princípios da governança digital. Busca-se, assim, identificar os limites dos sistemas atualmente utilizados, os riscos associados à opacidade decisória e à sobrecarga institucional, e os caminhos possíveis para uma atuação mais eficiente, justa e segura por parte da Polícia Federal no controle de armas de fogo no Brasil.

2. Fundamentação Teórica

Para compreender os desafios e oportunidades da digitalização no controle de armas de fogo pela Polícia Federal, é imprescindível estabelecer um sólido arcabouço teórico. Este capítulo se dedica a explorar os conceitos fundamentais da governança eletrônica, sua aplicação no âmbito dos sistemas de justiça e, mais especificamente, a emergência da justiça algorítmica (Gharaibeh et al, 2024). Essas perspectivas oferecem as lentes analíticas necessárias para uma discussão aprofundada sobre a intersecção entre tecnologia, administração pública e direitos fundamentais.

A modernização dos serviços públicos, impulsionada pelas Tecnologias da Informação e Comunicação (TICs), tem remodelado a interação entre o Estado e os cidadãos, além de otimizar a organização dos processos internos (Dias et al, 2019). No contexto do controle de armas de fogo, essa transformação é evidente nos sistemas informatizados utilizados pela Polícia Federal (PF), como o Sistema Nacional de Armas (SINARM) e o

SINARM-CAC. Ao digitalizar etapas antes manuais, esses sistemas geraram ganhos significativos em agilidade e padronização dos procedimentos.

Para compreender plenamente os desafios e as oportunidades desse cenário, é fundamental explorar dois conceitos complementares: governo eletrônico (e-government) e governança digital. O governo eletrônico, em sua essência, refere-se à digitalização dos serviços e processos administrativos com o objetivo primordial de aprimorar a eficiência da máquina pública (Guimarães & Medeiros, 2005). Por outro lado, a governança digital transcende essa visão, incorporando preocupações com a transparência, a responsabilização (*accountability*), a participação cidadã e a segurança da informação (Fabriz, Gomes & Mello, 2018).

A governança digital, conforme proposta por Fabriz, Gomes e Mello (2018), envolve não apenas a informatização de serviços, mas a incorporação de valores democráticos como transparência, participação e *accountability*. No contexto brasileiro, Vaz et al (2013) complementa essa visão ao defender que a transformação digital deve ser acompanhada de instrumentos efetivos de controle social e responsabilização institucional, especialmente quando envolve dados sensíveis ou decisões com impacto sobre direitos individuais.

Portanto, a governança digital não se restringe à mera adoção de sistemas eletrônicos; ela implica um compromisso com a gestão pública orientada por valores democráticos. Isso significa assegurar que a tecnologia seja empregada para fortalecer o controle social, a equidade no acesso aos serviços e a legitimidade das decisões públicas (Van der Meer, 2015). No contexto específico da Polícia Federal, isso exige que os sistemas utilizados para analisar pedidos de posse ou porte de armas não sejam apenas eficientes, mas também compreensíveis, auditáveis e seguros.

Com o avanço da digitalização, emergiu também o fenômeno da automação de decisões públicas, onde sistemas informatizados avaliam critérios e produzem decisões administrativas, como o deferimento ou indeferimento de pedidos (Dias et al, 2019). Embora esse processo confira rapidez, ele suscita preocupações significativas. A principal delas é a "justiça algorítmica", que descreve a tendência de decisões automatizadas baseadas em regras pré-programadas ou inteligência artificial, muitas vezes sem que o cidadão compreenda como a decisão foi formulada (McDowell, 1990). A chamada “justiça algorítmica”, que descreve decisões automatizadas opacas e sem justificativas compreensíveis, representa um risco direto à legalidade e à confiança social nos processos públicos (McDowell, 1990). No contexto brasileiro, Silveira (2021) alerta que a lógica algorítmica, quando não supervisionada, pode aprofundar desigualdades, reforçar discriminações preexistentes e reduzir a margem de contestação cidadã, especialmente quando as decisões são naturalizadas como técnicas ou neutras. Se os critérios empregados pelos sistemas forem opacos, pouco claros ou baseados em dados com vieses, há um risco considerável de decisões injustas, desiguais ou arbitrárias. Adicionalmente, na ausência de supervisão humana adequada, perde-se a capacidade de contextualizar o caso concreto ou

corrigir erros sistêmicos. Como alertam Bovens e Schillemans (2008), a falta de *accountability* em processos automatizados compromete diretamente a confiança da sociedade no Estado.

Outro pilar central da governança digital é a proteção de dados pessoais (Raposo et al, 2019). A Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018) estabeleceu critérios rigorosos para o tratamento de informações sensíveis no setor público. No âmbito do controle de armas, esses dados incluem antecedentes criminais, laudos psicológicos e informações de segurança. Sua gestão demanda cuidados técnicos e jurídicos especializados, especialmente quando envolvem decisões que afetam direitos fundamentais, como o acesso ao porte de arma.

Finalmente, a interoperabilidade entre sistemas e instituições configura-se como um desafio relevante (Cruz et al, 2020). A eficiência no controle de armas depende, em parte, da capacidade da Polícia Federal de acessar e cruzar informações provenientes de outras fontes, como o Poder Judiciário, o Ministério Público, os institutos de perícia e os órgãos estaduais de segurança pública. Para tal, é imperativo que existam padrões técnicos, protocolos de segurança e acordos formais de compartilhamento de dados, sempre em estrito respeito aos limites legais.

Em suma, o referencial teórico adotado neste artigo postula que a digitalização dos processos de controle de armas deve ser acompanhada por transparência decisória, segurança da informação, participação institucional e supervisão humana qualificada. A governança digital, nesse sentido, serve como uma lente crítica para avaliar se os sistemas utilizados pela Polícia Federal estão efetivamente contribuindo para uma gestão pública mais eficiente, segura e justa — ou se estão meramente replicando, de forma mais célere, os mesmos problemas estruturais persistentes.

3. Metodologia

Este artigo adota uma abordagem de ensaio teórico-crítico (Soares et al, 2018), com foco na análise conceitual e normativa dos sistemas informatizados de controle de armas de fogo utilizados pela Polícia Federal, sob a perspectiva da governança digital. A escolha dessa abordagem se justifica pela natureza do problema investigado, que envolve tanto aspectos jurídicos quanto institucionais e operacionais, exigindo uma compreensão aprofundada dos conceitos e de suas implicações na prática.

Trata-se de uma pesquisa qualitativa e exploratória, baseada em três pilares principais:

- Análise documental e normativa: revisão de legislações, decretos, portarias e instruções normativas que regem o controle de armas e o uso dos sistemas SINARM, SINARM-CAC e REGULA-CAC pela Polícia Federal. Dentre os documentos analisados, destacam-se a Lei nº 10.826/2003 (Estatuto do Desarmamento) e o Decreto nº 11.615/2023, além de

normativos internos relevantes para o tema. Esta análise busca identificar o arcabouço legal e regulatório que define a atuação da PF e a estrutura de seus sistemas digitais.

- Revisão de literatura temática: aprofundamento em conceitos-chave da governança digital, governo eletrônico, justiça algorítmica e proteção de dados pessoais. A fundamentação teórica foi construída a partir de autores renomados nessas áreas, a fim de embasar a análise crítica dos sistemas e seus desafios. A revisão busca estabelecer um diálogo entre as teorias e o cenário prático da digitalização do controle de armas.
- Análise crítica e síntese: por meio da interconexão entre o arcabouço normativo e os conceitos teóricos, o ensaio desenvolve uma análise crítica das implicações da digitalização para a eficiência, transparência e justiça do controle de armas. Esta etapa consiste na síntese e interpretação das informações coletadas, culminando na identificação dos desafios e na proposição de reflexões para o aprimoramento da governança digital na área.

Adicionalmente, a autora atua na área de controle de armas da Polícia Federal, o que confere ao estudo uma perspectiva aplicada, ainda que não empírica no sentido estrito. A vivência direta em unidades da instituição permitiu a identificação de limitações operacionais, gargalos administrativos e desafios práticos enfrentados no cotidiano, que foram reinterpretados à luz do arcabouço teórico adotado. Esse posicionamento institucional contribui para uma análise crítica mais contextualizada, embora as observações não constituam dados coletados sistematicamente nem representem posições oficiais da Polícia Federal.

A análise é conduzida com uma perspectiva crítica, buscando não apenas descrever os aspectos formais e operacionais dos sistemas informatizados de controle de armas, mas também problematizar suas implicações institucionais, jurídicas e democráticas à luz dos princípios da governança digital. O objetivo é oferecer subsídios para uma reflexão qualificada sobre os limites e possibilidades da digitalização no contexto da segurança pública, com especial atenção à transparência, à *accountability*, à proteção de dados e à equidade no acesso ao serviço público.

4. A Digitalização do Controle de Armas na Polícia Federal

Com a edição do Decreto nº 11.615/2023, a Polícia Federal assumiu parte das atribuições antes exclusivas do Exército Brasileiro no controle de Colecionadores, Atiradores e Caçadores (CACs). Essa transição envolveu não apenas a gestão administrativa, mas também a incorporação de um público até então vinculado ao SIGMA, sistema utilizado pelo Exército. A PF precisou desenvolver, em prazo reduzido, sistemas próprios — SINARM-CAC e REGULA-CAC — para recepcionar essas demandas.

A transferência, contudo, evidenciou inúmeras dificuldades práticas. A ausência de integração plena entre o SIGMA e os sistemas da PF gerou inconsistências cadastrais, duplicidade de registros e falhas na rastreabilidade. Servidores e cidadãos passaram a relatar

instabilidades constantes, serviços temporariamente indisponíveis e erros sistêmicos que atrasam análises e geram insegurança jurídica. Além disso, a interpretação e aplicação da nova legislação trouxeram dúvidas tanto para usuários quanto para operadores, já que a normatização da transição não acompanhou, com a mesma velocidade, as mudanças tecnológicas.

Esse cenário revela que a digitalização, embora necessária, não eliminou os gargalos do controle estatal de armas. Ao contrário, expôs com maior clareza a importância de uma governança digital robusta, baseada em interoperabilidade, clareza normativa e segurança jurídica, para que a transferência de atribuições do Exército à Polícia Federal se traduza em efetividade e confiança social.

A informatização dos processos administrativos relacionados ao controle de armas de fogo representou um marco importante na modernização da Polícia Federal. Antes sustentadas em fluxos manuais, planilhas e papel, as atividades de registro, fiscalização e análise de pedidos passaram a ser realizadas por meio de sistemas eletrônicos, com destaque para o Sistema Nacional de Armas (SINARM) e, mais recentemente, o SINARM-CAC e o REGULA-CAC, voltados ao controle de Colecionadores, Atiradores e Caçadores.

A migração de processos essencialmente analógicos para um ambiente totalmente informatizado alterou profundamente a rotina da instituição, gerando tanto avanços notáveis quanto desafios complexos. Essa digitalização se insere em um esforço mais amplo de modernização do Estado brasileiro, impulsionado por políticas de governo eletrônico e, mais recentemente, por diretrizes de governança digital Rodrigues & Cammarosano, 2022). No contexto da Polícia Federal, o uso desses sistemas visa não apenas acelerar o tempo de resposta às demandas da sociedade, mas também fortalecer o controle interno, reduzir fraudes, padronizar procedimentos e facilitar a fiscalização.

A digitalização dos serviços públicos tem sido uma diretriz estratégica em diversos órgãos da administração pública, e na Polícia Federal não foi diferente. O controle de armas de fogo, que antes dependia de processos essencialmente físicos, foi profundamente transformado com a implementação de sistemas eletrônicos, principalmente o Sistema Nacional de Armas (SINARM) e o SINARM-CAC, voltado aos Colecionadores, Atiradores e Caçadores. Essa mudança trouxe ganhos significativos, mas também revelou limitações operacionais importantes, especialmente frente à crescente demanda relacionada aos CACs.

O SINARM é o principal sistema utilizado pela Polícia Federal para o registro, controle e fiscalização de armas de fogo em poder de civis. Previsto originalmente pela Lei nº 10.826/2003, sua função é consolidar em uma base única todas as informações sobre as armas registradas no país, os seus proprietários e as condições legais para sua posse ou porte. O sistema centraliza dados como: número de série das armas, categoria, proprietário, endereço, validade do registro e movimentações associadas.

Com a reestruturação normativa ocorrida nos últimos anos — especialmente após o Decreto nº 11.615/2023 —, a PF também passou a controlar, parcialmente, os registros dos CACs, grupo que anteriormente era gerido exclusivamente pelo Exército por meio do SIGMA. Para isso, foi desenvolvido o SINARM-CAC e o REGULA-CAC, sistemas próprios para recepcionar as demandas dessa categoria, incluindo aquisição, renovação, registro e movimentação de armamentos. Ambos os sistemas têm interface *online*, com acesso via plataforma Gov.br, permitindo que o cidadão acompanhe o andamento de seus processos de forma remota. Internamente, as unidades da PF utilizam painéis de trabalho e módulos administrativos para análise e validação dos pedidos.

A transição parcial do controle de Colecionadores, Atiradores e Caçadores (CACs) do Exército (via SIGMA) para a Polícia Federal (PF) através do SINARM-CAC, impulsionada pelo Decreto nº 11.615/2023, apresenta desafios e oportunidades significativas para a governança digital. Anteriormente, o Exército gerenciava exclusivamente os registros dos CACs. Com essa mudança normativa, a PF, que já utiliza o SINARM para o controle de armas de civis , precisou desenvolver o SINARM-CAC para recepcionar as novas demandas dessa categoria.

Entre os desafios, destaca-se a necessidade de garantir a plena interoperabilidade entre o SINARM e o SIGMA. A fragmentação entre sistemas é apontada no ensaio como uma limitação operacional importante, impedindo análises de risco abrangentes e a checagem completa de antecedentes. A ausência de integração com bases de dados externas essenciais, como as do Poder Judiciário e Ministério Público, é um problema que se estende à relação com o SIGMA, dificultando o controle efetivo de armas e levando a decisões importantes baseadas em dados desatualizados ou incompletos. Faltam acordos formais, protocolos de segurança e padronização de dados para permitir a troca segura e automática de informações entre as instituições. Auditorias externas já corroboraram deficiências na integração entre o SINARM e outras bases de dados.

Por outro lado, essa transição oferece a oportunidade de consolidar uma visão mais integrada do controle de armas no país. Uma interoperabilidade efetiva entre SINARM e SIGMA poderia fortalecer o rastreamento de armas e proprietários, otimizando a fiscalização e a troca de informações cruciais para a segurança pública. A digitalização, que já trouxe ganhos significativos como a padronização de rotinas e a agilidade na análise para a PF , pode ser potencializada com a superação dos "silos digitais" existentes, construindo uma governança interinstitucional robusta. A efetivação dessa integração é crucial para que a digitalização do controle de armas na PF contribua para uma segurança pública mais efetiva e justa.

A transição da Polícia Federal para plataformas digitais no controle de armas, como o SINARM, o SINARM-CAC e o REGULA-CAC, trouxe avanços inegáveis, alinhando-se aos princípios da governança digital focados na eficiência e padronização. A digitalização permitiu a uniformização de procedimentos em nível nacional, agilizou o atendimento

através da interligação com bases de dados como CPF e CNH, e garantiu a rastreabilidade completa das ações e decisões, essencial para auditorias e revisões. Além disso, a inibição de fraudes documentais e o acesso remoto para acompanhamento de processos pelos cidadãos demonstram um esforço significativo em modernizar a gestão pública e ampliar a transparência e o acesso à informação.

Esses ganhos são compatíveis com os princípios da governança digital, que busca uma administração pública mais eficiente, segura e padronizada (Fabriz, Gomes & Mello, 2018). Além disso, a digitalização respondeu, em parte, à pressão por mais agilidade no atendimento aos cidadãos, especialmente diante do crescimento expressivo de novos registros, impulsionado pelo aumento dos CACs.

Apesar dos avanços, os sistemas enfrentam limitações operacionais significativas, principalmente quando observados do ponto de vista de quem trabalha diretamente com eles nas unidades da Polícia Federal. Essas limitações demonstram que a digitalização, embora necessária e positiva, não é uma solução mágica. Sistemas informatizados, quando mal geridos, podem reproduzir ou até agravar problemas antigos da administração pública, como a lentidão, a opacidade e a insegurança jurídica (Fórum Brasileiro de Segurança Pública, 2022). A governança digital, nesse sentido, exige mais do que tecnologia: requer planejamento, supervisão, investimento e avaliação contínua.

A transição do controle de armas de um modelo predominantemente manual para um ambiente digital representou um avanço institucional para a Polícia Federal. No entanto, à medida que os sistemas informatizados passaram a assumir funções cada vez mais complexas — incluindo a análise de critérios, geração de pareceres automáticos e até indeferimentos baseados em filtros sistêmicos — surgiram novos desafios que vão além da dimensão técnica. Muitos desses obstáculos dizem respeito à qualidade da governança digital adotada.

A análise teórica revela que esses avanços podem ser mitigados por desafios críticos, especialmente diante do exponencial crescimento do público CAC. Um dos principais problemas teóricos enfrentados é a opacidade dos critérios utilizados para o deferimento ou indeferimento de solicitações. Em diversas situações, o requerente é informado apenas de que seu pedido foi indeferido "com base nos critérios do sistema", sem que lhe seja apresentada uma justificativa detalhada. Isso compromete o direito à informação, à ampla defesa e ao contraditório.

Essa ausência de clareza nas decisões automatizadas caracteriza um risco típico da chamada "justiça algorítmica" — em que sistemas decidem, mas não explicam (McDowell, 1990). Quando a lógica interna do sistema é inacessível até mesmo aos servidores que o operam, há um sério risco de arbitrariedade digitalizada, que pode ser ainda mais difícil de contestar do que decisões humanas mal fundamentadas. A literatura aponta que se os critérios empregados pelos sistemas forem opacos, pouco claros ou baseados em dados com vieses, há um risco considerável de decisões injustas, desiguais ou arbitrárias. Quando a

lógica interna do sistema é inacessível até mesmo aos servidores que o operam, há um sério risco de arbitrariedade digitalizada, que pode ser ainda mais difícil de contestar do que decisões humanas mal fundamentadas. A falta de *accountability* em processos automatizados compromete diretamente a confiança da sociedade no Estado (Rocha, 2011).

A instabilidade recorrente dos sistemas, com potenciais quedas e lentidão, pode comprometer tanto o trabalho interno da Polícia Federal quanto o acesso do cidadão, gerando acúmulo de demandas e retrabalho. Soma-se a isso a defasagem no processamento de dados e, crucialmente, a falta de integração com outras bases de dados essenciais, como as do Judiciário, Ministério Público e Polícia Civil. Essa limitação de interoperabilidade impede análises de risco abrangentes e a checagem de antecedentes, dificultando o controle efetivo de armas e levando a decisões importantes baseadas em dados desatualizados ou incompletos.

Outro desafio está relacionado à dependência excessiva dos sistemas informatizados. Embora a automação traga ganhos operacionais, ela não deve substituir completamente a análise humana, especialmente em casos que envolvem interpretação jurídica, análise de risco ou contexto social (Vieira & Barreto, 2019).

A governança digital exige um equilíbrio: os sistemas devem auxiliar a decisão, mas não eliminar a possibilidade de revisão humana qualificada, especialmente em situações-limite, como pedidos de porte de arma com histórico de ameaças ou contextos de violência doméstica.

Além disso, a carência de capacitação técnica dos servidores que atuam diretamente nos processos pode comprometer a interpretação correta dos alertas, das pendências sistêmicas e das regras de negócio ocultas no sistema.

Adicionalmente, os sistemas SINARM, SINARM-CAC e REGULA-CAC lidam com informações sensíveis, como antecedentes criminais, laudos psicológicos, endereços residenciais e informações sobre segurança pessoal. A má gestão desses dados, seja por falhas de segurança, seja por uso indevido, pode gerar graves consequências para os cidadãos.

Nesse contexto, a Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018) impõe obrigações legais à administração pública, incluindo a necessidade de consentimento (quando cabível), limitação de acesso, finalidade específica e registros de tratamento. A conformidade dos sistemas da PF com a LGPD ainda é um ponto que carece de maior regulamentação e visibilidade pública.

A implementação da Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018) nos sistemas SINARM, SINARM-CAC e REGULA-CAC da Polícia Federal enfrenta desafios específicos que demandam atenção. Embora os sistemas lidem com informações sensíveis como antecedentes criminais, laudos psicológicos e endereços residenciais , a conformidade com a LGPD carece de maior regulamentação e visibilidade pública. É crucial discutir como a PF tem garantido a necessidade de consentimento para o tratamento desses

dados (quando cabível), a limitação de acesso apenas a usuários autorizados e a finalidade específica para a qual cada informação é coletada e utilizada. Além disso, a ausência de transparência sobre a arquitetura de segurança dos sistemas e a falta de auditorias externas regulares geram preocupações sobre a segurança da informação (Toledo & Pessoa, 2023), especialmente em um contexto em que *hackers* e organizações criminosas podem ter interesse em dados de portadores de armas. A proposição de auditorias externas periódicas com controle social e a nomeação de um encarregado específico de proteção de dados para os sistemas de armas, juntamente com a criação de rotinas auditáveis de acesso, são passos essenciais para reforçar a segurança e a confiança social, garantindo que a gestão desses dados sensíveis respeite plenamente os direitos fundamentais dos cidadãos.

Auditorias realizadas por órgãos de controle externos também corroboram a existência dessas deficiências. Foram apontadas falhas no controle de armas, como a concessão de registros para pessoas com históricos criminais ou mesmo menores de idade, e a insuficiência na verificação da habitualidade de atiradores. No contexto dos sistemas da PF, as verificações indicaram deficiências na integração entre o SINARM e outras bases de dados, além da ausência de normativos internos atualizados para as novas atribuições (Santos, 2025).

O controle efetivo de armas depende da capacidade da PF de acessar dados atualizados de outras instituições, como o Poder Judiciário (ex. medidas protetivas, condenações), o Ministério Público (investigações em curso), as polícias civis (boletins de ocorrência) e o Exército (registros antigos de CACs).

Contudo, essa interoperabilidade entre sistemas é limitada ou inexistente em muitos casos. Faltam acordos formais, protocolos de segurança, padronização de dados e infraestrutura tecnológica para permitir a troca segura e automática de informações. Sem isso, a análise de risco fica comprometida, e decisões importantes podem ser tomadas com base em dados desatualizados ou incompletos.

Por fim, o modelo 100% digital, embora eficaz para muitos usuários, pode marginalizar aqueles que não possuem acesso adequado à *internet*, conhecimento técnico ou apoio jurídico, criando uma barreira digital ao acesso a direitos fundamentais (Oliveira Amorim et al, 2025). Para mitigar esse problema, além da manutenção de canais presenciais ou híbridos de atendimento com linguagem acessível, como já apontado, é imperativo que a governança digital seja acompanhada de políticas públicas ativas de inclusão digital. Isso envolve iniciativas como a expansão do acesso à *internet* em áreas remotas, programas de capacitação digital para populações com baixa escolaridade e em situação de vulnerabilidade social, e a garantia de que as ferramentas digitais sejam desenvolvidas com design inclusivo, pensando na usabilidade por diversos públicos.

A equidade no acesso ao serviço público exige que a digitalização não se torne um privilégio tecnológico, mas sim uma ferramenta que democratize o acesso e a participação de todos os cidadãos, sem reforçar desigualdades sociais preexistentes. Populações em áreas

remotas, com baixa escolaridade ou em situação de vulnerabilidade social podem encontrar dificuldades para acessar os sistemas, realizar correções ou entender os procedimentos. Para garantir a equidade no acesso ao serviço público, é necessário que a digitalização venha acompanhada de canais de suporte, alternativas presenciais e linguagem acessível nos sistemas e nos documentos gerados.

O uso de sistemas informatizados pela Polícia Federal no controle de armas representa, portanto, um avanço importante, especialmente diante do aumento exponencial da demanda — em grande parte impulsionada pelo crescimento do público CAC. A digitalização trouxe benefícios reais, como agilidade e padronização, mas ainda enfrenta limites estruturais, jurídicos e operacionais.

Sob a ótica da governança digital, os sistemas SINARM, SINARM-CAC e REGULA-CAC precisam evoluir para garantir transparência, segurança, supervisão humana e integração entre órgãos públicos. Sem esses pilares, o risco é de que a tecnologia amplifique desigualdades, dificulte o acesso à justiça e enfraqueça a confiança social no controle de armas.

Diante desse cenário, é possível afirmar que a superação dos desafios apontados exige mais do que ajustes pontuais: requer um compromisso institucional com uma governança digital robusta, orientada por princípios democráticos e técnicas de gestão pública inteligente. A explicabilidade algorítmica, por exemplo, precisa deixar de ser um ideal abstrato e se tornar uma prática cotidiana. Os sistemas SINARM, SINARM-CAC e REGULA-CAC devem apresentar de forma clara, compreensível e auditável os critérios utilizados para deferimento ou indeferimento de solicitações, garantindo que os cidadãos compreendam os fundamentos das decisões que lhes afetam diretamente. Essa transparência não é apenas desejável, mas essencial para o exercício do contraditório, da ampla defesa e da correção de eventuais falhas sistêmicas.

Além disso, é imprescindível estabelecer instâncias de supervisão humana qualificada, sobretudo nos casos mais complexos ou sensíveis. A automação deve ser entendida como uma ferramenta de apoio, e não como substituta da análise contextual. Isso implica na capacitação contínua dos servidores que operam os sistemas, na criação de núcleos técnicos multidisciplinares para revisão de casos críticos e no fortalecimento do discernimento institucional frente a situações atípicas. A sensibilidade humana continua sendo indispensável na tomada de decisões que envolvem riscos à vida, segurança pessoal ou contextos de vulnerabilidade.

Outro eixo fundamental de aprimoramento é a interoperabilidade entre sistemas e instituições. O controle efetivo de armas de fogo exige que a Polícia Federal tenha acesso ágil e seguro a dados judiciais, investigativos e administrativos que permitam a avaliação precisa do perfil de risco do requerente. A ausência de integração entre SINARM, SINARM-CAC, SIGMA e bases de dados do Judiciário e do Ministério Público compromete a eficácia do processo decisório e pode expor vítimas e a própria sociedade a riscos evitáveis. Portanto,

é necessário investir na construção de uma arquitetura de dados integrada, baseada em protocolos de segurança, acordos interinstitucionais e atualização tecnológica permanente.

No campo da proteção de dados, a conformidade com a Lei Geral de Proteção de Dados precisa ser efetiva e transparente. Os sistemas que tratam informações sensíveis sobre antecedentes criminais, laudos psicológicos e endereços devem ser submetidos a auditorias externas periódicas, com controle social e registros formais de tratamento. A nomeação de um encarregado específico de proteção de dados para os sistemas de armas e a criação de rotinas auditáveis de acesso podem reforçar a segurança da informação sem comprometer a eficiência dos processos.

Ainda que a digitalização represente um avanço em termos de acessibilidade, é fundamental considerar os riscos da exclusão digital institucionalizada. Nem todos os cidadãos têm acesso pleno à *internet*, familiaridade com os sistemas ou recursos técnicos para lidar com plataformas digitais complexas. Nesse sentido, a governança digital inclusiva exige que se mantenham canais presenciais ou híbridos de atendimento, com linguagem acessível, suporte técnico e versões simplificadas dos sistemas que permitam a plena participação de públicos diversos, especialmente os mais vulneráveis.

Por fim, a construção de uma governança digital verdadeiramente democrática exige o monitoramento contínuo dos próprios algoritmos e processos automatizados. A criação de comitês internos de ética algorítmica, a atualização periódica dos parâmetros de decisão conforme mudanças legais e jurisprudenciais, e a publicação de relatórios de impacto digital são práticas recomendáveis para garantir a integridade e a evolução dos sistemas. A governança de dados, nesse sentido, não pode ser apenas técnica: precisa ser ética, transparente e comprometida com os direitos fundamentais.

Essas diretrizes, quando implementadas em conjunto, têm o potencial de consolidar um modelo de controle de armas que não apenas se modernize tecnologicamente, mas que também respeite os valores democráticos, assegure direitos, reduza desigualdades e promova a confiança da sociedade no Estado brasileiro.

5. Discussão

A implementação dos sistemas SINARM, SINARM-CAC e REGULA-CAC pela Polícia Federal representa um caso emblemático dos paradoxos da governança digital no Brasil. Enquanto a literatura acadêmica celebra os potenciais transformadores da digitalização na administração pública (Fabriz, Gomes & Mello, 2018; Guimarães & Medeiros, 2005), a realidade operacional revela uma tensão fundamental entre a promessa de eficiência tecnológica e a manutenção de princípios democráticos fundamentais.

Os desafios teóricos enfrentados pela digitalização do controle de armas na Polícia Federal, sob a ótica da governança digital, podem ser sistematizados em três eixos principais.

Primeiramente, a opacidade algorítmica e a justiça algorítmica representam um gargalo fundamental, manifestando-se na ausência de clareza sobre os critérios decisórios dos sistemas SINARM, SINARM-CAC e REGULA-CAC, o que compromete o direito à informação, à ampla defesa e ao contraditório, levando a decisões automatizadas sem justificativas compreensíveis.

Em segundo lugar, a fragmentação e a limitada interoperabilidade de dados emergem como um obstáculo crítico, impedindo a integração efetiva com bases externas como Judiciário, Ministério Público e SIGMA/Exército, resultando em análises de risco incompletas e decisões baseadas em informações desatualizadas.

Por fim, a tensão entre automação e supervisão humana, e os riscos de vieses algorítmicos, destaca a necessidade de um equilíbrio entre a eficiência tecnológica e o discernimento humano, alertando para a possibilidade de que os sistemas reproduzam ou amplifiquem desigualdades e discriminações preexistentes, caso não haja uma governança de dados ética e transparente.

A análise dos sistemas revela um paradoxo central: a digitalização, teoricamente promotora de transparência, pode na prática gerar maior opacidade. Os indeferimentos automáticos baseados em "critérios do sistema" constituem o que se pode denominar de caixa-preta decisória, um fenômeno onde a automação obscurece, ao invés de esclarecer, os fundamentos das decisões administrativas. Esta opacidade não é meramente um problema técnico, mas uma questão de legitimidade democrática. McDowell (1990) já alertava para os riscos da justiça algorítmica, mas a prática na Polícia Federal demonstra que esses riscos se materializam de forma ainda mais perversa quando nem mesmo os operadores do sistema compreendem sua lógica interna. Diferentemente de uma decisão administrativa tradicional, onde o servidor pode explicar seus critérios, o algoritmo se torna um burocrata digital incontestável e incompreensível.

Para aprofundar as implicações éticas e legais da "caixa-preta decisória", é imperativo que a discussão sobre a "justiça algorítmica" transcenda a mera constatação da opacidade para explorar as barreiras concretas à contestação judicial de decisões automatizadas. A ausência de justificativas detalhadas para indeferimentos, fundamentadas apenas em "critérios do sistema" , não só viola o direito à informação, à ampla defesa e ao contraditório, mas também exige o desenvolvimento de mecanismos processuais que permitam desvendar a lógica interna desses algoritmos. Torna-se crucial, portanto, discutir a necessidade de regulamentação específica que imponha transparência algorítmica e estabeleça requisitos de explicabilidade para sistemas utilizados em decisões públicas que afetam direitos fundamentais, como o controle de armas. A literatura contemporânea sobre justiça algorítmica aponta para a urgência de auditorias algorítmicas independentes e para a definição clara de responsabilidades legais em caso de vieses ou erros sistêmicos, uma vez que a falta de *accountability* compromete diretamente a confiança da sociedade no Estado.

A promessa de imparcialidade da automação, no entanto, é frequentemente mitigada pelo risco de reprodução e amplificação de vieses implícitos nos dados de entrada ou nos próprios critérios algorítmicos. No contexto do controle de armas de fogo, esses vieses podem se manifestar de diversas formas. Por exemplo, se os dados históricos utilizados para treinar os sistemas SINARM, SINARM-CAC e REGULA-CAC refletirem um padrão desigual de policiamento ou de registros criminais que impacta desproporcionalmente certas regiões geográficas ou grupos socioeconômicos, o algoritmo pode, inadvertidamente, perpetuar ou intensificar essas disparidades. Critérios de avaliação que dependam de indicadores socioeconômicos ou de endereços específicos podem levar a vieses geográficos, dificultando ou impedindo o acesso ao registro de armas para residentes de áreas periféricas ou de menor renda, mesmo que preencham os requisitos legais. Similarmente, vieses raciais ou de gênero, presentes em dados históricos ou em decisões humanas pré-digitalização, podem ser incorporados ao algoritmo, resultando em decisões injustas ou arbitrárias para determinados grupos. A opacidade desses vieses algorítmicos torna sua identificação e correção um desafio ainda maior, comprometendo a equidade e a não discriminação nas decisões automatizadas da Polícia Federal.

A governança digital autêntica exige mais do que eficiência; demanda explicabilidade algorítmica. A ausência de transparência nos critérios decisórios não representa apenas uma falha técnica, mas uma regressão democrática digitalizada. O Estado não pode se esconder atrás da complexidade tecnológica para justificar decisões que afetam direitos fundamentais. Neste sentido, a limitada interoperabilidade entre os sistemas da Polícia Federal e outras bases de dados governamentais expõe uma contradição estrutural da governança digital brasileira. Promete-se um Estado conectado e eficiente, mas a realidade revela silos digitais que reproduzem, em formato eletrônico, as mesmas fragmentações burocráticas do Estado analógico.

Esta fragmentação não é neutra. Quando a Polícia Federal toma decisões sobre porte de armas sem acesso a informações atualizadas sobre medidas protetivas ou investigações em curso, não está apenas operando com dados incompletos, mas potencialmente colocando vidas em risco. A ausência de integração com bases do Judiciário, por exemplo, pode resultar na concessão de porte de arma para indivíduos com histórico de violência doméstica não capturado pelos sistemas da PF. A governança digital efetiva pressupõe governança interinstitucional, e a mera digitalização de processos isolados não constitui transformação digital genuína. O caso dos sistemas de controle de armas demonstra como a ausência de uma arquitetura de governança de dados integrada pode comprometer a própria finalidade do controle estatal.

O uso de sistemas digitais como instrumentos de decisão pública, embora associado ao ideal de eficiência, frequentemente mascara disputas de poder e legitimações institucionais que ocorrem sob a superfície técnica. Como destaca Cesarino (2023), os sistemas de automação do Estado não são neutros, mas refletem disputas políticas e escolhas

normativas que moldam as condições de acesso a direitos, como o controle de armas no Brasil.

A crescente automação dos processos decisórios na Polícia Federal levanta questões fundamentais sobre o papel do julgamento humano na era digital. Os sistemas automatizados, embora eficientes no processamento de casos padronizados, carecem da capacidade de contextualização necessária para lidar com situações complexas ou atípicas. Esta limitação se torna crítica em contextos em que a vida humana está em jogo. Uma decisão automatizada que concede porte de arma a um potencial agressor, ou que o nega a uma vítima de ameaças, pode ter consequências irreversíveis. A ilusão da neutralidade algorítmica mascara o fato de que todo sistema automatizado incorpora, em sua programação, escolhas e valores humanos.

A governança digital não deve ser sinônimo de desumanização da administração pública. A eficiência sistêmica não pode ser perseguida às custas da capacidade de discernimento e contextualização humana. É necessário desenvolver modelos híbridos que combinem a agilidade da automação com a sabedoria da supervisão humana qualificada. Paralelamente, os sistemas SINARM, SINARM-CAC e REGULA-CAC processam dados extremamente sensíveis, cuja exposição pode comprometer a segurança física dos cidadãos. Contudo, a conformidade com a LGPD permanece nebulosa, e a arquitetura de segurança dos sistemas não é transparente nem submetida a auditorias externas regulares.

Esta opacidade na segurança dos dados é particularmente problemática em um contexto em que *hackers* e organizações criminosas têm interesse direto em informações sobre portadores de armas. A falsa sensação de segurança proporcionada pela digitalização pode na verdade aumentar a vulnerabilidade dos cidadãos. A governança digital responsável exige transparência sobre segurança sem comprometer a própria segurança. A sociedade tem o direito de saber como seus dados sensíveis são protegidos, especialmente quando sua exposição pode resultar em riscos físicos. A ausência de auditoria externa e prestação de contas sobre segurança de dados constitui uma lacuna crítica na governança digital da PF.

Paradoxalmente, a digitalização dos serviços pode gerar exclusão digital institucionalizada. A transição para plataformas exclusivamente digitais pode marginalizar populações vulneráveis, criando uma barreira digital para o acesso a direitos fundamentais. Esta exclusão é particularmente problemática no contexto do controle de armas, onde o acesso ao porte pode ser uma questão de segurança pessoal. Cidadãos em situação de vulnerabilidade social ou geográfica podem ser impedidos de exercer seus direitos simplesmente por não dominarem as competências digitais necessárias. A governança digital inclusiva não pode ser um privilégio tecnológico, e a digitalização de serviços públicos deve ser acompanhada de políticas ativas de inclusão digital e manutenção de canais alternativos de acesso.

A análise dos sistemas de controle de armas da Polícia Federal revela que a governança digital no Brasil ainda opera sob uma lógica tecnocrática que privilegia

eficiência sobre transparência, automação sobre deliberação, e padronização sobre equidade. Esta abordagem representa uma modernização conservadora que reproduz, em formato digital, as mesmas patologias da burocracia tradicional. A verdadeira transformação digital da administração pública demanda uma reorientação paradigmática que coloque os princípios democráticos no centro do processo de digitalização, incluindo transparência algorítmica como princípio não negociável, integração sistêmica baseada em governança interinstitucional robusta, supervisão humana qualificada como complemento indispensável à automação, segurança de dados transparente e auditável, e inclusão digital como política pública prioritária.

A governança digital efetiva não é apenas sobre tecnologia, mas sobre democracia digital. Os sistemas de controle de armas da Polícia Federal têm o potencial de se tornarem um modelo de governança digital democrática, mas isso exige uma transformação profunda que vá além da mera informatização de processos existentes. A digitalização do controle de armas pela Polícia Federal representa tanto uma oportunidade quanto um desafio para a consolidação de uma governança digital genuinamente democrática no Brasil. O caminho para essa consolidação passa necessariamente pela superação da visão tecnocrática atual em favor de uma abordagem que coloque os valores democráticos no centro do processo de transformação digital do Estado.

Para que a digitalização do controle de armas de fogo pela Polícia Federal transcenda a mera eficiência e alcance uma governança digital verdadeiramente democrática, é imperativo aprofundar a compreensão e a aplicação prática da "supervisão humana qualificada" e de um modelo robusto de "governança de dados". A supervisão humana qualificada deve materializar-se na formação de equipes multidisciplinares e na capacitação contínua dos servidores, permitindo a revisão estratégica de casos sensíveis – como indeferimentos ou situações de alto risco – que demandam contextualização e discernimento que os algoritmos, por si só, não podem oferecer. Paralelamente, uma governança de dados ideal exige não apenas a conformidade com a Lei Geral de Proteção de Dados (LGPD) , mas a promoção de interoperabilidade e integração robustas entre o SINARM/SINARM-CAC e bases de dados externas cruciais, como as do Poder Judiciário e Ministério Público, garantindo a qualidade, segurança e finalidade no tratamento das informações. Tal abordagem sistêmica é fundamental para superar a fragmentação do Estado digital e assegurar que as decisões automatizadas sejam justas, transparentes e alinhadas aos direitos fundamentais.

Este estudo não realizou coleta empírica com usuários ou operadores dos sistemas SINARM/SINARM-CAC, o que representa uma limitação. Pesquisas futuras podem incluir entrevistas com servidores, análise documental de decisões automatizadas e estudos comparados com outros sistemas públicos de controle sensível, como imigração, trânsito ou saúde.

6. Conclusão

A digitalização dos processos de controle de armas de fogo pela Polícia Federal, por meio dos sistemas SINARM, SINARM-CAC e REGULA-CAC, é um passo significativo na modernização da administração pública brasileira, impulsionada pelo crescimento exponencial da demanda de CACs. Os benefícios de agilidade, padronização e rastreabilidade são evidentes e alinham-se aos princípios de uma governança digital eficiente. Contudo, a discussão aprofundada revelou que a mera adoção tecnológica, sem uma governança digital robusta, pode criar paradoxos e comprometer os valores democráticos fundamentais.

O ponto mais crítico reside na opacidade dos critérios decisórios automatizados, que transformam a digitalização em uma "caixa-preta decisória". Essa falta de explicabilidade algorítmica não é um problema técnico menor, mas uma questão de legitimidade democrática, minando o direito à informação e ao contraditório e corroendo a confiança na instituição. A justiça algorítmica, nesse contexto, pode levar a decisões arbitrárias e incompreensíveis, demonstrando uma regressão democrática digitalizada onde o Estado se resguarda na complexidade tecnológica.

A opacidade da "caixa-preta decisória" e a limitada integração dos sistemas têm impactos diretos e concretos. Por exemplo, imagine um cidadão que teve seu pedido de posse de arma indeferido pelo SINARM-CAC. O sistema retorna a mensagem genérica de "indeferido com base nos critérios do sistema", sem detalhar qual requisito não foi atendido ou qual dado levou à recusa. Esse cenário impede o cidadão de entender o motivo real da decisão, tornando impossível apresentar uma defesa efetiva ou corrigir eventuais informações equivocadas, ferindo seu direito ao contraditório. Sem essa transparência, o requerente fica à mercê de uma decisão algorítmica incompreensível e, muitas vezes, impossível de contestar administrativamente, replicando uma "arbitrariedade digitalizada".

Outro cenário hipotético ilustra a falha na integração de dados. Considere um indivíduo que, após um histórico de violência doméstica, obteve uma medida protetiva expedida pelo Poder Judiciário em outro estado. Se o SINARM-CAC não possui integração em tempo real com as bases de dados judiciais, a Polícia Federal pode conceder um novo registro ou renovar um porte de arma para essa pessoa, colocando em risco a segurança da vítima. Essa lacuna de interoperabilidade impede análises de risco abrangentes e a checagem de antecedentes completa, resultando em decisões importantes baseadas em dados desatualizados ou incompletos. Similarmente, um servidor da PF pode se deparar com um sistema lento e instável , incapaz de carregar informações cruciais sobre um solicitante, atrasando o processo e gerando acúmulo de trabalho e retrabalho , enquanto informações essenciais para a segurança, como investigações em curso no Ministério Público, permanecem inacessíveis.

Além disso, a limitada interoperabilidade dos sistemas da Polícia Federal com outras bases de dados governamentais expõe a fragmentação do Estado digital. Decisões cruciais sobre controle de armas são tomadas com base em informações incompletas, o que pode resultar em riscos reais à segurança pública, como a concessão de porte a indivíduos com histórico de violência. A governança digital autêntica exige governança interinstitucional e uma arquitetura de dados integrada, que supere os "silos digitais" e permita um fluxo contínuo de informações para análises de risco abrangentes e precisas.

A crescente automação também levanta questionamentos sobre o papel do julgamento humano. Embora os sistemas sejam eficientes em casos padronizados, eles não substituem a capacidade de contextualização e discernimento humano, especialmente em situações complexas que envolvem a vida e a segurança das pessoas. A governança digital não pode desumanizar a administração pública; ela deve buscar um equilíbrio entre a agilidade da automação e a sabedoria da supervisão humana qualificada, garantindo que as decisões reflitam não apenas a lógica algorítmica, mas também a sensibilidade para casos atípicos.

A proteção de dados sensíveis e a conformidade com a LGPD, embora cruciais para a segurança dos cidadãos, ainda carecem de transparência e auditorias externas regulares. A opacidade na segurança dos dados, em um setor tão sensível como o controle de armas, aumenta a vulnerabilidade dos cidadãos a riscos externos. Por fim, a digitalização exclusiva dos serviços pode gerar exclusão digital, marginalizando populações vulneráveis que não possuem acesso ou familiaridade com o ambiente virtual, o que impede o acesso a direitos fundamentais e reforça a desigualdade social.

Concluindo, para que a digitalização do controle de armas na Polícia Federal atinja seu potencial máximo e contribua para uma segurança pública mais efetiva e justa, é indispensável uma reorientação paradigmática. A governança digital deve ir além da mera informatização de processos, abraçando uma abordagem que coloque a transparência algorítmica, a integração sistêmica robusta, a supervisão humana qualificada, a segurança de dados auditável e a inclusão digital como pilares inegociáveis. Somente assim a Polícia Federal poderá consolidar um controle de armas que não apenas seja eficiente, mas também democrático, equitativo e capaz de fortalecer a confiança social no Estado. Esse é o caminho para uma verdadeira democracia digital no Brasil.

Referências

Bovens, M., & Schillemans, T. ’t Hart, P.(2008). Does public accountability work. *An assessment tool. Public Administration*, *86*(1), 225-242.

Castells, M. (2011). *The rise of the network society*. John Wiley & sons.

McDowell, L. I. N. D. A. (1990). The Condition of Postmodemity: An Enquiry into the origins of Cultural Change.

Cesarino, L. (2023). Novas mídias, nacionalidade e o caleidoscópio antigênero. *Gênero e Linguagem* , *17* (1), 102-110.

Chen, Y. C., & Hsieh, T. C. (2014). Big data for digital government: Opportunities, challenges, and strategies. *International journal of public administration in the digital age (IJPADA)*, *1*(1), 1-14. Van der Meer, J. (2015). *Public sector innovation and the role of digital governance*. Springer.

Cruz, M., Delgado, M., Bernardini, F., Nunes, V., & Bastos, C. A. (2020, June). Interoperabilidade e Integração de Sistemas e Dados para Apoio à Tomada de Decisão pela Gestão da Prefeitura de Volta Redonda-RJ: Perspectivas e Desafios. In *Workshop de Computação Aplicada em Governo Eletrônico (WCGE)* (pp. 148-155). SBC.

de Oliveira Amorim, B., de Sales, J. G. G., de Souza, F. E. X., de Jesus, M. S., Oliveira, K. D. S. P., Seabra, F. C. D. S. C., ... & Ramos, P. R. (2025). Tecnologias digitais e cidadania: desafios e oportunidades para a inclusão digital no Brasil-uma revisão sistemática da literatura. *REVISTA DELOS*, *18*(63), e3527-e3527.

Dias, T. F., Sano, H., & Medeiros, M. F. M. D. (2019). Inovação e tecnologias da comunicação e informação na administração pública.

do Carmo, J. S., de Souza Rodrigues, M. A., & Silva, B. C. (2025). Governança Digital e Modernização da Polícia Judiciária: Implementação de Procedimentos Policiais Eletrônicos como Ferramentas de Eficiência e Otimização de Recursos. In *Temas Emergentes Da Nova Administração Pública Brasileira* (Vol. 1, pp. 8-30). Editora Científica Digital.

do Nascimento, A. F., Viana, J. M. B., de Lira, M. T. M., Lima, A. P. S., de Melo, A. V. M. S., Aleixo, B. A., ... & Maia, R. (2025). Sistemas de informação para tomada de decisão administrativa: uma revisão bibliográfica: uma revisão bibliográfica. *Revista Universitária Brasileira*, *3*(1).

Fabriz, S. M., Gomes, A. R. V., & Mello, G. R. de. (2018). Governança Eletrônica: Uma Análise Bibliométrica dos Periódicos Nacionais e Internacionais. *Contabilidade Gestão E Governança*, *21*(3), 320–338. https://doi.org/10.51341/1984-3925_2018v21n3a2

Guimarães, T. de A., & Medeiros, P. H. R.. (2005). A relação entre governo eletrônico e governança eletrônica no governo federal brasileiro. *Cadernos EBAPE.BR*, *3*(4), 01–18. https://doi.org/10.1590/S1679-39512005000400004

da Silveira, S. A., Souza, J., Cassino, J. F., & Machado, D. F. (2022). *Colonialismo de dados: como opera a trincheira algorítmica na guerra neoliberal*. Autonomia literária.

Rocha, A. C. (2011). Accountability in Public Administration: Theoretical Models and Approaches. *Contabilidade Gestao e Governanca*, *14*(2), 82-97.

Rodrigues, C. B., & Cammarosano, F. G. F. (2022). Governança digital: avanços e desafios do processo administrativo eletrônico no Brasil. *Revista de Direito Internacional e Globalização Econômica*, *9*(09), 198-219.

Santos, L. D. R. (2025). Capacidades essenciais e dinâmicas necessárias no controle de armas de fogo pela Polícia Federal.

Soares, S. V., Picolli, I. R. A., & Casagrande, J. L. (2018). Pesquisa bibliográfica, pesquisa bibliométrica, artigo de revisão e ensaio teórico em administração e contabilidade. *Administração: ensino e pesquisa*, *19*(2), 308-339.

Toledo, C., & Pessoa, D. (2023). O uso de inteligência artificial na tomada de decisão judicial. *Revista de Investigações Constitucionais*, *10*(1), e237.

Vaz, J. C., Ribeiro, M. M., & Matheus, R. (2013). Desafios para a Governança Eletrônica e Dados Governamentais Abertos em Governos Locais. In *WTRANS13-Workshop de Transparência em Sistemas*.

Vieira, J. B., & Barreto, R. D. S. (2019). *Governança, gestão de riscos e integridade. Enap*.