Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.258
ISSN 2595-4717

Diego Serpa[1]
ORCiD 0009-0001-6161-2647

TRANSFORMAÇÃO DIGITAL DA INTELIGÊNCIA NACIONAL BRASILEIRA

https://doi.org/10.58960/rbi.2024.19.258

Serpa, Diego. 2024. "Transformação digital da inteligência nacional brasileira". *Revista Brasileira de Inteligência* (ABIN), n. 19: e2024.19.258. https://doi.org/10.58960/rbi.2024.19.258.

Recebido em 19/11/2024
Aprovado em 25/11/2024
Publicado em 31/12/2024

[1] Servidor público. Mestre em Direito do Estado (UFPR). Pesquisador associado ao Núcleo de Pesquisa em Inteligência (NUPI) da Escola de Inteligência (Esint).

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.258
ISSN 2595-4717

TRANSFORMAÇÃO DIGITAL DA INTELIGÊNCIA NACIONAL BRASILEIRA

Resumo

Este artigo examina o impacto da transformação digital na inteligência nacional do Brasil. Destacam-se os reflexos da introdução das tecnologias digitais e a consequente redefinição das dinâmicas geopolíticas. Exploram-se os efeitos dessas mudanças no setor público brasileiro, com ênfase nos riscos subjacentes e nas implicações para a segurança das pessoas e das instituições. Conforme a análise, a transformação digital tem o potencial de aprimorar as capacidades do Sistema Brasileiro de Inteligência (Sisbin), aumentando a integração e a vantagem decisória gerada pelo sistema, enquanto exige o endereçamento de temas como a cibersegurança, a proteção de dados e a privacidade. Por fim, o artigo discute uma estratégia para a transformação digital do Sisbin, avaliando os desafios e as oportunidades relacionados.

Palavras-chave: Serviço de Inteligência (Brasil), Transformação digital, Sistema Brasileiro de Inteligência (Sisbin), Agência Brasileira de Inteligência (ABIN).

DIGITAL TRANSFORMATION OF THE BRAZILIAN NATIONAL INTELLIGENCE

Abstract

This article discusses the impact of digital transformation on Brazil's national intelligence. It highlights the effects of introducing digital technologies and the consequent redefinition of geopolitical dynamics. The paper explores the effects of these changes on Brazil's public sector, emphasizing the underlying risks and implications for national security. According to the analysis, digital transformation has the potential to enhance the capabilities of the Brazilian Intelligence System (Sisbin), increasing integration and the decision-making advantage provided by the system, while requiring that the authorities address issues such as cybersecurity, data protection, and privacy. Finally, the article discusses a strategy for the digital transformation of Sisbin, evaluating the related challenges and opportunities.

***Keywords**: Intelligence Service (Brasil), Digital transformation, Brazilian Intelligence System (Sisbin), Brazilian Intelligence Agency (ABIN).*

TRANSFORMACIÓN DIGITAL DE LA INTELIGENCIA NACIONAL BRASILEÑA

Resumen

Este artículo analiza el impacto de la transformación digital en la inteligencia de Brasil. Destácanse los efectos de la introducción de tecnologías digitales y la consiguiente redefinición de la dinámica geopolítica. Explora los efectos de estos cambios en el sector público de Brasil, haciendo hincapié en los riesgos subyacentes y las implicaciones para la seguridad nacional. Según el análisis, la transformación digital tiene el potencial de mejorar las capacidades del Sistema Brasileño de Inteligencia, aumentando la integración y la ventaja en la toma de decisiones que proporciona el sistema, mientras exige respuestas sobre temas como la ciberseguridad, la protección de datos y la privacidad. Finalmente, analiza una estrategia para la transformación digital del Sisbin, evaluando los retos y oportunidades relacionados.

***Palabras clave**: Servicio de Inteligencia (Brasil), Transformación digital, Sistema Brasileño de Inteligencia (Sisbin), Agencia Brasileña de Inteligencia (ABIN).*

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.258
ISSN 2595-4717

Introdução

Nas últimas décadas, a "transformação digital" tem redesenhado a geopolítica e a economia globais. Esse termo é definido como o conjunto de transformações desencadeado pela adoção de tecnologias digitais, com alterações profundas nos modos de vida (Vial 2019; Śledziewska e Włoch 2021; Mitkiewicz 2024). A Era Digital em que vivemos distingue-se pela centralidade crescente da ciência, da tecnologia e dos sistemas de inovação digitalizados para a produção, a circulação e o consumo de valor criado pelo trabalho intelectual em rede (Cepik e Brancher 2022).

Tais mudanças fazem parte de um fenômeno mais amplo que afeta a sociedade em geral, que passa a ser caracterizada como uma "sociedade de rede". Essa estrutura social tem como atividade econômica central a produção, o processamento e a distribuição de informações por meio das tecnologias digitais de informação e comunicação (TICs), impactando as percepções de espaço, com o ciberespaço, e de tempo, com a comunicação em tempo real e os mercados ininterruptos (Castells 2009; Castells 2009-2010). No plano geopolítico, surge um novo tipo de ameaça para a segurança de pessoas e instituições: as ameaças cibernéticas, exploradas por atores estatais e não estatais para afirmar seus interesses (Zegart 2022).

Apesar das desigualdades no acesso às tecnologias digitais no Brasil, as redes sociais influenciam a política nacional e, mesmo no campo, as TICs já automatizam os processos de produção (OCDE 2018; Mercuri e Lima-Lopes 2020; Cozendey et al. 2021; Brasil 2022; Pereira e Castro 2022; Ribeiro et al. 2022; Mitkiewicz 2024). O volume extraordinário de dados digitais (*big data*) e a capacidade de analisálos inclusive por meio de inteligência artificial (IA) criam tanto oportunidades quanto ameaças, exigindo respostas estratégicas dos setores público e privado (Lima et al. 2023).

No campo da administração de empresas, a transformação digital é vista como uma oportunidade para inovar as cadeias de geração de valor, embora demande gerir desafios relacionados a tecnologia, pessoas, processos e cultura (Vial 2019; Lang 2021). No setor público, por sua vez, além de otimizar a prestação de serviços, essa transformação aproxima governo e cidadãos, ampliando a transparência e fomentando novas formas de participação social (Cozendey et al. 2021). O processo, no entanto, pode agravar vulnerabilidades sociais e tecnológicas, e requer uma governança global que aborde questões éticas, como o uso de IA e aspectos de cibersegurança (OCDE 2020 ; Cepik e Brancher 2023).

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.258
ISSN 2595-4717

Para a inteligência nacional, a transformação digital amplia o escopo e o espaço de competição geopolítica. Por um lado, gera possibilidades de coleta e de análise de dados em uma nova escala; por outro, intensifica riscos de contrainteligência e preocupações com direitos de privacidade e proteção de dados. A Agência Brasileira de Inteligência (ABIN), como órgão central do Sistema Brasileiro de Inteligência (Sisbin), está liderando iniciativas para integrar o sistema por meio de serviços digitais e capacitá-lo para enfrentar esses desafios, o que inclui a criação de serviços de comunicação e de compartilhamento seguro de dados (Brasil 2024f). Essa iniciativa tem o potencial de transformar significativamente a atividade de inteligência e o valor gerado para a sociedade brasileira. Não obstante, seu êxito demandará um processo de gerenciamento de riscos minucioso e contínuo.

Por meio do método de análise documental (Bowen 2009; Lakatos e Marconi 2017), com apoio do método de análise de políticas públicas (Secchi 2013; Dunn 2017), este artigo examina os potenciais efeitos da transformação digital da inteligência nacional brasileira em três seções: a transformação digital no setor público brasileiro e seus reflexos para a segurança; a transformação digital do Sisbin; e, por fim, as oportunidades e os desafios associados.

Transformação digital no setor público brasileiro: reflexos para a segurança de pessoas e instituições

Partindo de um cenário de iniciativas desintegradas e localizadas, o governo federal brasileiro lançou um plano ambicioso de implantação do governo digital. Reconheceu-se a necessidade de abandonar a abordagem de governo eletrônico, que se concentrava na mera replicação digital de serviços públicos tradicionais. Em contraste, a abordagem de governo digital busca integrar tecnologias digitais em todos os processos decisórios, maximizando os impactos positivos dos investimentos nas TICs e buscando garantir coerência e coordenação de políticas. O uso estratégico de tecnologias digitais e de dados é entendido como crucial para que as organizações do setor público ofereçam serviços aprimorados, que possam resultar em maior satisfação e confiança dos cidadãos no governo (OCDE 2018; Lima et al. 2023 ; Mitkiewicz 2024).

Uma peça fundamental para o plano do governo brasileiro foi a criação da plataforma Gov.br em 2019. A plataforma representou um passo significativo em termos de obtenção centralizada de serviços públicos (*one-stop shop*) e já oferece quase cinco mil serviços. Após um rápido salto de maturidade, o país tornou-se referência: alcançou, entre 198 países, o segundo lugar no ranking de GovTech do Banco Mundial e a 14ª posição, entre 193, no índice de serviços online da ONU (Mitkiewicz 2024).

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.258
ISSN 2595-4717

O processo não tem sido isento de desafios. Um deles diz respeito à própria inclusão digital da sociedade brasileira, seja por falta de acesso à internet, seja por carência de competências de letramento digital (Cozendey et al. 2021). Em 2023, 65% das escolas públicas rurais não dispunham de conexão de alta velocidade e 15,7% dos domicílios não contavam com qualquer forma de acesso à internet (CETIC.BR 2024a). Além disso, apenas 30% da população brasileira possui habilidades digitais básicas, como copiar ou mover um arquivo ou pasta (Brasil 2024e). Outra dificuldade é relativa à privacidade e proteção de dados pessoais. Mais de 80% dos usuários de internet no Brasil estão preocupados com o uso de seus dados biométricos por órgãos governamentais (CETIC.BR 2024b). Um dos fatores que tem contribuído para essa preocupação é a implementação vagarosa da Lei Geral de Proteção de Dados Pessoais nas instituições públicas (Ribeiro et al. 2022; Mitkiewicz 2024).

Em articulação com esses desafios, há elementos políticos que dialogam com a transformação digital do Estado brasileiro. No âmbito governamental, disputas quanto à alocação de recursos, à divisão de competências, e a forma de coordenar ações para garantir a proteção dos dados dos cidadãos podem atrasar a implementação ou comprometer a eficiência das iniciativas. Todos esses elementos agravariam um quadro de "desigualdade digital", em que uma parcela da população está excluída de acessar serviços públicos essenciais pela internet (Ribeiro et al. 2022; Lima et al. 2023).

Associado às preocupações sobre proteção de dados, há um grande desafio de cibersegurança. O redesenho dos serviços públicos em torno de tecnologias digitais torna-os dependentes da infraestrutura de hardware e software e da prestação de serviços especializados, ampliando a suscetibilidade a falhas e a vulnerabilidades. Além disso, quantidades significativas de dados pessoais dos cidadãos e de dados estratégicos passam a ficar suscetíveis a ataques.

Desde 2020, o Estado brasileiro já sofreu, por exemplo, vazamento de credenciais de acesso a sistemas do Ministério da Saúde, expondo dados pessoais de mais de 200 milhões de pessoas; ataques de ransomware ao Superior Tribunal de Justiça e à Biblioteca Nacional; e, mais recentemente, um caso de phishing que redundou em desvio de R$ 3,5 milhões do Sistema Integrado de Administração Financeira (Siafi) (Cambricoli 2020; Souza 2020; G1 2021; CNN BRASIL 2024).

As ameaças de cibersegurança e os atores envolvidos têm uma dimensão geopolítica significativa. A parcela mais avançada dos grupos que as exploram, conhecidos como "APTs" (sigla em inglês para "ameaças avançadas persistentes", *advanced persistant threats*), frequentemente opera em favor

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.258
ISSN 2595-4717

de interesses estatais. Os Estados também exploram diretamente vulnerabilidades cibernéticas para fins econômicos e políticos. Chegam a público alegações de ciberespionagem econômica ou de interferência estrangeira em processos eleitorais (Espanha 2019). Determinados serviços de inteligência valem-se das empresas e da infraestrutura de TIC baseadas em seus países para executar ações de inteligência ofensivas contra autoridades, organizações ou cidadãos estrangeiros[1].

Além disso, a definição de políticas de cibersegurança envolve decisões estratégicas sobre soberania digital, influenciadas por pressões internacionais e por diferentes visões de atores governamentais sobre a dependência em relação a tecnologias estrangeiras (Belli et al. 2023; Aguiar 2023). A soberania digital se torna um tema crítico na medida em que condiciona a capacidade do Estado de fazer cumprir suas decisões e preservar seus interesses no ciberespaço. Governança de dados, capacidades de produção de software e hardware (especialmente de semicondutores), infraestrutura de TIC e criptografia são elementos que refletem não só aspectos econômicos, mas também a posição política do Brasil em relação a grandes potências, como Estados Unidos e China, que frequentemente utilizam sua influência sobre o ecossistema digital como ferramenta de política externa (Cepik e Brancher 2023).

A transição tecnológica e suas implicações geopolíticas, portanto, afetam a atividade de inteligência nacional em decorrência da evolução das capacidades disponíveis aos diversos atores, bem como da ampliação de seu escopo de atuação. Nesse contexto, os sistemas de inteligência, incluído o brasileiro, verificam a necessidade de transformar suas estruturas e processos por meio das tecnologias digitais.

Transformação digital do Sisbin

A transformação digital impacta significativamente os serviços de inteligência: em sua forma de atuação, no cumprimento de suas missões tradicionais e mesmo no conjunto de ameaças a serem endereçadas. Um dos aspectos mais relevantes é a proliferação de dados digitais, que apresenta oportunidades e ameaças para a atividade de inteligência.

Em perspectiva positiva para a atividade, grandes volumes de dados podem ser coletados e explorados por meio de técnicas como as de inteligência de fontes abertas (*open source intelligence*, Osint) para analisar ameaças e subsidiar o processo decisório (Guterman 2023). Em contrapartida, a ex-

1 Um exemplo foi o caso de espionagem contra a Petrobras, revelado em 2013 (FANTÁSTICO 2013).

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.258
ISSN 2595-4717

ploração eficiente desses dados exige investimentos relevantes em infraestrutura digital, no desenvolvimento de competências da força de trabalho e na implementação de capacidades de *analytics* e de IA (Blanchard e Taddeo 2023; SCSP 2024).

Ademais, essa transformação também demanda mudanças em aspectos de cultura organizacional relacionados ao sigilo, à compartimentação e ao secretismo, num cenário em que os fenômenos chegam ao conhecimento do Estado e do grande público praticamente ao mesmo tempo (Smeets e Lin 2018; Hockenhull 2022). Além disso, a transformação digital desencadeia a emergência de novos tipos de ameaças e de atores, incluindo ciberataques sofisticados, campanhas de desinformação por IA, e a ascensão de atores não-estatais (Kollars 2023; SCSP 2024). Essas ameaças não raro são de caráter transnacional e requerem novas formas de colaboração e de compartilhamento de inteligência (CSIS 2021; SCSP 2024).

Para enfrentar esses desafios, argumenta-se que os serviços de inteligência devem abraçar a transformação digital de suas próprias organizações, o que demanda não só a adoção de tecnologias de ponta, mas a reconfiguração de estruturas e culturas organizacionais (CSIS 2021; SCSP 2024). O processo envolveria a realização de parcerias com atores privados na vanguarda da inovação; a simplificação de modelos de aquisição e de implementação de soluções de TIC; e mesmo o desenvolvimento de abordagens mais abertas, ágeis e colaborativas na execução do ciclo de produção de inteligência (CSIS 2021; SCSP 2024; USSC 2023).

Nesse sentido, em contextos democráticos, é essencial que os serviços conduzam o processo prezando pela transparência e pela construção de confiança com a sociedade. Assim, devem confrontar preocupações sobre privacidade e dar respostas assertivas sobre como as novas tecnologias estão sendo utilizadas na coleta de dados (CSIS 2021; Guterman 2023; Blanchard e Taddeo 2023). De forma similar ao restante do setor público, a transformação digital das organizações de inteligência também pode auxiliar nesse aspecto, ao facilitar o mapeamento e o monitoramento de processos; ao prover informações gerenciais em tempo real para o corpo diretivo; e ao gerar dados que podem ser utilizados em medidas de transparência e de conformidade para o público interno, externo e para os organismos de controle (Lima et al. 2023; Mitkiewicz 2024).

No Brasil, a política de inteligência nacional é levada a efeito pelo Sisbin e pela ABIN, seu órgão central, ambos criados pela Lei nº 9.883 de 1999. A criação do Sisbin na virada do milênio – oito anos após a extinção do sistema

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.258
ISSN 2595-4717

anterior, o Sistema Nacional de Informações (Sisni) – coloca-o num contexto diretamente afetado pela transformação digital.

As tecnologias digitais impactam o escopo e o potencial de concretizar a missão legal do Sistema de "fornecer subsídios ao Presidente da República nos assuntos de interesse nacional" (art. 1º) e suas responsabilidades de obter, analisar e disseminar informações para o processo decisório do Poder Executivo federal e proteger conhecimentos sensíveis (art. 2º, § 1º; art. 4º, I e II). Essas tecnologias também têm efeitos positivos sobre a transparência, a conformidade e o controle externo, pois permitem a implementação de requisitos de rastreabilidade, auditabilidade e visibilidade na produção de inteligência.

No caso do Sisbin, o controle e a fiscalização externos do sistema devem ser exercidos pelo Poder Legislativo, na forma da lei (art. 6º). Esse controle pode compreender "todo o ciclo da inteligência, entre as quais as [fases] de reunião, por coleta ou busca, análise de informações, produção de conhecimento, e difusão, bem como a função de contrainteligência e quaisquer operações a elas relacionadas", conforme a resolução CN nº 2 de 2013 que criou a Comissão Mista de Controle das Atividades de Inteligência (CCAI).

Não obstante o contexto tecnológico em que foi criado, o Sisbin tem convivido, nas mais de duas décadas após sua fundação, com relacionamentos informais e baixa integração entre as instituições que o compõem (49 em 2024). A CCAI recebe críticas por sua atuação esporádica, limitada a reagir a crises, em vez de fiscalizar contínua e preventivamente as atividades do sistema (Gonçalves e Bedritichuk 2024). Essas circunstâncias decorreriam da transição entre o período autoritário e a democracia no Brasil, que ainda impõe ao sistema de inteligência desafios de institucionalização, legitimidade e efetividade (Cepik 2005; Gill 2012; Bruneau 2015; Cepik 2021).

De um ponto de vista prático, o Sisbin enfrenta dificuldades de interoperabilidade tecnológica entre os sistemas de seus órgãos e instituições, o que prejudica a integração das bases de dados, a eficiência na troca de informações e a extração de valor em termos de vantagem decisória ou de proteção de conhecimentos sensíveis. O intercâmbio de dados ocorre de forma pouco eficiente e com baixo nível de rastreabilidade e controle. Os dados são armazenados em silos isolados pertencentes às diferentes instituições. São utilizados métodos de intercâmbio que, embora relativamente seguros, têm pouca agilidade e dependem de relacionamentos pessoais. Essa estrutura de funcionamento possui altos custos de transação para a troca de informações e exige emprego intensivo de pessoal qualificado.

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.258
ISSN 2595-4717

Iniciativas como a criação da "Rede Cronos" no âmbito do Subsistema de Inteligência de Segurança Pública (Portaria MJSP nº 36, de 29 de março de 2021) e os investimentos correlatos do Ministério da Justiça e Segurança Pública em soluções para compartilhamento de documentos, por exemplo, restringiram-se à digitalização do intercâmbio de documentos entre órgãos de segurança pública. A transformação digital dos processos de produção de inteligência em nível estratégico permanece incipiente.

Visando a superar essas disfunções, o Poder Executivo federal promoveu uma ampla reforma do regulamento do Sisbin por meio do Decreto nº 11.693, de 6 de setembro de 2023. A reforma aposta em um modelo coordenado e cooperativo, no qual a integração entre os componentes e, consequentemente, o aperfeiçoamento da atividade de inteligência brasileira e de seu controle sejam facilitados e induzidos pela adoção de soluções e padrões digitais unificados. Nesse sentido, destacam-se as competências da ABIN de promover a cooperação e a integração das atividades de inteligência entre as instituições que compõem o sistema; coordenar a produção de inteligência integrada; e, principalmente, estabelecer padrões de governança de dados e oferecer soluções digitais para comunicação e compartilhamento de informações (art. 10, I, III, IV, VI, X e XI). Ressaltam-se, além disso, as competências comuns dos integrantes do Sisbin de executar ações de obtenção, integração, processamento e compartilhamento de dados (art. 11, I e II).

O decreto previu procedimentos para o ingresso de membros federados, vinculados aos estados e aos municípios. Com a regulamentação desse tipo de ingresso, o sistema tende a se expandir e a gestão das trocas informacionais e dos relacionamentos em nível técnico tende a se tornar ainda mais complexa, o que demanda a transformação digital dos processos, sob pena de obsolescência ou de agravamento das disfunções.

Existem soluções comerciais estrangeiras de ponta voltadas para a gestão e a produção integradas de inteligência. Entretanto, a implementação de plataformas comerciais, embora possa constituir ganhos concretos no curto prazo, acarreta riscos à segurança e à soberania digital do Brasil, especialmente no atual contexto de competição entre potências, conforme mencionado na seção anterior. De forma a enfrentar esses riscos, a ABIN, propondo-se a liderar a transformação do Sisbin, firmou em março de 2024 um plano de transformação digital (PTD) com o Ministério da Gestão e Inovação em Serviços Públicos (MGI) (Brasil 2024f). São cinco os objetivos indicados:

- prover serviço de comunicação segura para os órgãos e entidades da Administração Pública Federal, especialmente os do Sisbin, de modo a

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.258
ISSN 2595-4717

proteger as comunicações sensíveis do Estado brasileiro;

- transformar o Sisbin em um sistema orientado a dados, cujas decisões e produtos se baseiem primordialmente em evidências;

- propiciar que a atividade de inteligência integre dados de forma ampla e abrangente, alavancando o valor de seus produtos;

- garantir que a produção do Sisbin seja devidamente gerenciada, com rastreabilidade, auditabilidade e visibilidade; e

- garantir conformidade com as normas aplicáveis ao Sisbin.

O plano tem como proposição central a de que o Sisbin terá êxito no fornecimento de inteligência ao Poder Executivo federal caso o sistema seja efetivamente integrado por meio de serviços digitais. Essa proposição é fundamentada nas seguintes hipóteses.

1. Conectar o Sisbin melhorará a quantidade e a qualidade de seus produtos e serviços: serviços digitais de integração facilitarão a ingestão e o compartilhamento de dados e de outros insumos providos pelos integrantes, por outros órgãos e entidades e por fontes abertas. Isso diminuirá as assimetrias informacionais e funcionais entre os integrantes e qualificará a oferta de produtos e serviços pelo sistema, favorecendo seu consumo pelo Poder Executivo federal e pelo próprio Sisbin.

2. Transformar os processos aumentará a produtividade e o engajamento dos agentes públicos dos órgãos e das entidades do sistema: o redesenho dos processos para o contexto digital e a implementação de capacidades de automação e de IA diminuirá os erros, o retrabalho e a quantidade de tarefas burocráticas e repetitivas. Isso aumentará a produtividade e o engajamento dos agentes públicos.

3. O maior valor dos produtos e serviços do sistema aumentará a disposição de seus integrantes para fornecerem insumos uns aos outros, criando um círculo virtuoso: com o aumento das vantagens de se integrar e de interagir efetivamente no âmbito do sistema, os integrantes serão incentivados a retornar outros insumos aos demais, cumprindo a primeira hipótese e criando um círculo de incentivos positivos.

Essas três hipóteses, caso realizadas, aumentarão os recursos disponíveis (produtividade dos agentes públicos e quantidade e qualidade dos insumos),

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.258
ISSN 2595-4717

a produtividade geral do sistema e o valor público gerado para a sociedade brasileira em termos de vantagem decisória e de proteção de conhecimentos sensíveis. De acordo com a estratégia adotada pela ABIN, para concretizar essas hipóteses, será necessário implementar as seguintes capacidades:

- interoperabilidade;
- governança de dados;
- gestão de riscos;
- inteligência artificial;
- segurança das comunicações e segurança cibernética;
- rastreabilidade, auditabilidade e visibilidade;
- infraestrutura de TIC flexível, escalonável e soberana; e
- financiamento contínuo.

Para o primeiro ciclo, o plano de transformação digital da ABIN prevê a entrega de dois serviços públicos inovadores: um aplicativo de comunicação (texto, voz, vídeo e arquivos) protegida por algoritmos criptográficos do Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações, órgão da ABIN (Cepesc/ABIN); e uma plataforma que possibilite a produção, o compartilhamento e a integração de produtos e de serviços de inteligência pelos órgãos e entidades do Sisbin, também com criptografia própria. Essas duas soluções têm o potencial de favorecer novas proposições de valor para o sistema ao possibilitar o crescimento exponencial das trocas entre os órgãos e instituições do Sisbin (Lang 2021; Plekhanov et al. 2023). Seu êxito, não obstante, demanda a abordagem de desafios corriqueiros em processos de transformação digital.

Oportunidades e desafios

Enquanto os benefícios da transformação digital do Sisbin têm cunho mais específico, seus desafios são similares aos encontrados por outras organizações. As oportunidades estão relacionadas, principalmente, à consolidação do Sisbin enquanto sistema efetivo, da qual poderiam ser extraídos três benefícios principais: (i) explorar o potencial dos dados sob a custódia do governo brasileiro para prover vantagem decisória ao Poder Executivo; de for-

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.258
ISSN 2595-4717

ma mais específica, (ii) prover soluções ao processo de transformação digital do Estado brasileiro para mitigar riscos e fortalecer a soberania digital do Brasil; e, por fim, (iii) aumentar a confiabilidade do sistema perante o Estado e a sociedade. Os desafios, por sua vez, dizem respeito à (a) manutenção de estratégia coerente e (b) de patrocínio na hierarquia de governo, além de (c) fatores normativos, (d) tecnológicos, (e) humanos e (f) financeiros. Ademais, há considerações (g) sociais e éticas relacionadas à atividade de inteligência num contexto democrático.

A oportunidade de explorar o potencial dos dados sob a custódia do governo para prover vantagem decisória (i) tem relação com os objetivos indicados no plano de transformação digital da ABIN (Brasil 2024f) e com a hipótese (1) de que conectar o Sisbin melhorará a quantidade e a qualidade de seus produtos e serviços. Para isso, o Sisbin deve integrar dados em posse do governo, a exemplo do catálogo de dados inserido na iniciativa Conecta Gov. br (Brasil 2024a), a dados de fontes abertas, o que demanda capacidades de interoperabilidade, governança de dados e IA. Assim, o sistema poderá utilizar o valor dos dados agregados para pautar suas próprias decisões, inclusive explorando o potencial dos dados e da IA (*data-driven decision making* e *AI-driven decision making*), e prover produtos que forneçam vantagem ao processo de decisão do Poder Executivo.

Nesse sentido, a integração de dados reduziria a necessidade de ações de inteligência para obtenção de dados já disponíveis noutros órgãos ou entidades do sistema ou em fontes abertas, permitindo concentrar as ações mais complexas na busca de dados realmente indisponíveis e, por consequência, melhorando a qualidade do gasto público. Da mesma maneira, permitiria utilizar informações de fontes diversas de forma oportuna para prover consciência situacional na tomada de decisão em situações de crise.

Uma segunda oportunidade (ii) diz respeito à possibilidade de prover soluções para mitigar riscos à segurança cibernética e à segurança das informações e das comunicações do Estado. O êxito na transformação digital do Sisbin pode se refletir em soluções de comunicação segura e de tratamento seguro de informações sigilosas com potencial de uso em toda a Administração Pública Federal, favorecendo a soberania digital brasileira. Nesse sentido, destacam-se as exigências de fortalecer as capacidades do Cepesc/ABIN e de garantir a implementação das soluções em infraestrutura de TIC flexível, escalonável e soberana, cumprindo a diretriz *cloud first* do governo brasileiro (Brasil 2024d). Igualmente, evidencia-se a necessidade de que a inteligência nacional esteja inserida nas discussões sobre definição de padrões criptográficos, nuvem de governo, nuvem soberana e redes privativas de comuni-

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.258
ISSN 2595-4717

cação para a administração pública, de maneira a informar sobre os riscos envolvidos (Brasil 2024b).

Ainda no campo das oportunidades, (iii) a transformação digital do Sisbin poderá oferecer respostas mais efetivas ao controle externo exercido pela CCAI e, em última instância, à própria sociedade brasileira ao implementar, desde o início do desenvolvimento das soluções e da concepção dos processos digitais, requisitos de rastreabilidade, auditabilidade e visibilidade na produção de inteligência. Esse elemento pode contribuir para superar as dificuldades de legitimidade e de institucionalização do sistema (Cepik 2021) previamente aludidos.

Por outro lado, para levar a efeito a transformação digital do Sisbin, será necessário superar alguns desafios geralmente associados a esse tipo de iniciativa. Em primeiro lugar, (a) é necessário garantir que a estratégia seja coerente e esteja submetida a monitoramento e atualização contínuas (Mitkiewicz 2024). A pactuação do PTD da ABIN com o MGI e o monitoramento realizado por esse ministério são boas medidas nesse sentido (Brasil 2024f). Para a continuidade de patrocínio (b) pela gestão da ABIN e pelas autoridades superiores do Executivo, por sua vez, é indispensável a articulação entre as equipes responsáveis na Agência, seu corpo diretivo e as autoridades ministeriais.

No plano normativo (c), é necessário garantir que a iniciativa respeite as disposições aplicáveis e que estas acompanhem o desenvolvimento tecnológico e os riscos daí advindos. São de especial interesse, nesse sentido, as disposições do Gabinete de Segurança Institucional (GSI) sobre o tratamento de informação sigilosa, em especial aquelas referentes ao uso de criptografia e aos requisitos mínimos de segurança para computação em nuvem. Já no plano tecnológico (d), a ABIN terá de fortalecer a interoperabilidade para permitir a integração entre sistemas legados e bases de dados diversas e superar silos informacionais (Lang 2021). Podem facilitar esse processo iniciativas governamentais como a infraestrutura nacional de dados, "um conjunto de normas, políticas, arquiteturas, padrões [...], com vistas a promover o uso estratégico dos dados em posse dos órgãos e das entidades do Poder Executivo federal" (Brasil 2024c).

Os desafios de aspecto humano (e) dizem respeito tanto à resistência à mudança quanto à carência de competências digitais. Em regra, as pessoas sentem-se desconfortáveis com a mudança de processos com os quais já estão habituados. Essa resistência seria resultado da falta de comunicação clara sobre os benefícios da mudança ou do medo do desconhecido. A ca-

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.258
ISSN 2595-4717

rência de competências digitais também é significativa. Muitos profissionais podem não ter tido acesso a treinamentos adequados para acompanhar a evolução tecnológica. Isso cria uma lacuna de competências que impede a plena implementação das soluções e dos processos redesenhados (Lang 2021; Lima 2023).

Para superar esses desafios, é essencial investir em gestão da mudança, em capacitação contínua e em recrutamento especializado (Alvarenga et al. 2020; Lang 2021; Lima 2023). Envolver os agentes públicos desde o início do processo de mudança e oferecer suporte contínuo são medidas que podem ser eficazes para reduzir a resistência. É necessário conduzir um plano de comunicação sobre os objetivos e benefícios da transformação digital, destacando como a automação de processos pode liberar tempo para atividades de maior valor agregado e melhorar o produto final da atividade de inteligência. Na área de capacitação, projetos de letramento digital são fundamentais para preparar a força de trabalho para as exigências tecnológicas emergentes, permitindo que os agentes públicos se sintam mais seguros e capacitados para atuar em um ambiente digital. Além disso, não se pode prescindir de recrutar profissionais que já contem com competências avançadas, seja por meio de requisição, quando cabível, seja por meio de concurso público.

No aspecto financeiro (f), a transformação digital da inteligência convive com algumas circunstâncias que demandam esforços inovadores. Em primeiro lugar, o investimento inicial para desenvolvimento de soluções é relativamente elevado. Em segundo, como em qualquer iniciativa de transformação digital, é difícil determinar em quanto tempo esse investimento retornará em valor público para a sociedade (Lima 2023; Mitkiewicz 2024). Esse aspecto torna-se ainda mais complexo considerando o escopo de atuação da atividade de inteligência e a dificuldade de mensurar seu valor. Assim, é essencial que a Agência desenvolva e implemente modelos de financiamento extraorçamentário para as iniciativas de transformação digital de forma a garantir que os recursos não fiquem sujeitos a eventuais contingenciamentos ou à anualidade orçamentária.

Por fim, há considerações sociais e éticas (g) relacionadas à atividade de inteligência num contexto democrático. A facilitação ao acesso de dados pessoais dos cidadãos por meio dos serviços digitais pode ser interpretada pela sociedade como incentivo ao vigilantismo, à espionagem doméstica ou ao monitoramento em massa, recrudescendo a percepção de carência de legitimidade que já afeta o Sisbin. Para contrapor essa percepção, é crucial que a transformação digital do sistema destaque os requisitos de rastreabilidade, auditabilidade e visibilidade que serão implementados desde a concepção

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.258
ISSN 2595-4717

desses serviços digitais e que favorecerão o controle externo e judicial da motivação e da finalidade dos atos dos agentes públicos.

Esses mesmos requisitos deverão nortear a implementação de capacidades de IA, por exemplo, para evitar que os algoritmos reproduzam formas de discriminação e para permitir o controle e a explicabilidade de suas respostas (Ribeiro et al. 2022). Uma preocupação relevante é o potencial de os sistemas de IA perpetuarem e amplificarem preconceitos já existentes. Se os dados usados para treinar um algoritmo de IA contiverem preconceitos, a solução provavelmente produzirá resultados tendenciosos, o que pode levar à discriminação.

Ademais, a complexidade inerente dos algoritmos de IA muitas vezes torna difícil entender como as soluções chegam a uma determinada resposta. Essa falta de transparência pode minar a confiança e dificultar a responsabilização. Por fim, a enorme quantidade de dados necessária para treinar e operar sistemas de IA levanta preocupações sobre a segurança de dados e o potencial de uso indevido de informações pessoais. É fundamental, nesses aspectos, garantir que o desenvolvimento e a implementação de IA para o Sisbin sigam as disposições aplicáveis da LGPD e incorporem as premissas e as diretrizes éticas definidas pelo governo brasileiro por meio de iniciativas como o Plano Brasileiro de Inteligência Artificial (Brasil 2024g).

Conclusões

A transformação digital do Sisbin é essencial para atender às novas exigências e dinâmicas da Era Digital. Transformar tecnologia, pessoas, processos e cultura dos órgãos e entidades do sistema tem o potencial de prover o Estado de vantagens decisórias e proteger o conhecimento sensível brasileiro.

Não obstante, desafios como segurança cibernética, resistência interna e carência de competências e de capacidades digitais ainda são significativos. Superar essas barreiras exige iniciativas claras de gestão da mudança, capacitação contínua e um modelo cooperativo para o Sisbin. É igualmente crucial garantir transparência e rastreabilidade nas ações do Sistema, visando construir a confiança da sociedade e atender às premissas de controle democrático. A implementação de tecnologias inovadoras, como a inteligência artificial, deve ser pautada por princípios éticos, prevenindo abusos e garantindo o respeito aos direitos humanos.

A transformação digital da inteligência nacional no Brasil deve ser conduzida com uma visão de longo prazo, envolvendo investimentos contínuos em

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.258
ISSN 2595-4717

infraestrutura e processos digitais, recrutamento e qualificação de pessoas e modelos inovadores de financiamento. Com isso, o Sisbin estará mais preparado para enfrentar os desafios da Era Digital, tornando-se eficiente, seguro e dando respostas às necessidades estratégicas da sociedade brasileira.

Referências

Aguiar, Thais Helena. 2023. *Políticas de segurança cibernética no Brasil: de onde viemos e para onde vamos*. Montevidéu: LACNIC. Acesso em 22 de outubro de 2024. https://www.lacnic.net/innovaportal/file/6974/1/politicas-de-seguranca-cibernetica-no-brasil-de-onde--viemos-e-para-onde-vamos-thais-helena-aguiar-pt.pdf.

Alvarenga, Ana, Florinda Matos, Radu Godina e João C. O. Matias. 2020. "Digital transformation and knowledge management in the public sector," *Sustainability* 12 (14): 5824. https://doi.org/10.3390/su12145824.

Belli, Luca, Bruna Diniz Franqueira, Erica Bakonyi, Larissa Chen, Natalia de Macedo Couto, Sofia Chang, Nina da Hora e Walter B. Gaspar. 2023. *Cibersegurança: uma visão sistêmica rumo a uma proposta de Marco Regulatório para um Brasil digitalmente soberano*. Rio de Janeiro: FGV Direito Rio. Acesso em 22 de outubro de 2024. https://repositorio.fgv.br/server/api/core/bitstreams/ece57a28-74ff-4bae--ab92-ad45c7bd1272/content.

Blanchard, Alexander e Mariarosaria Taddeo. 2023. "The ethics of artificial intelligence for intelligence analysis: a review of the key challenges with recommendations," *Digital Society* 2 (12). https://doi.org/10.1007/s44206-023-00036-4.

Bowen, Glenn. A. 2009. "Document analysis as a qualitative research method," *Qualitative Research Journal* 9 (2): 27-40. https://doi.org/10.3316/QRJ0902027.

Brasil. 2022. *Estratégia Brasileira para a Transformação Digital (E-Digital) - Ciclo 2022-2026*. Brasília: Governo Digital. Acesso em 22 de outubro de 2024. https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosestrategiadigital/e-digital_ciclo_2022-2026.pdf.

Brasil. 2024a. "Conecta Gov.br." Brasília: Governo Digital. Acesso em 22 de outubro de 2024. https://www.gov.br/governodigital/pt-br/legislacao/conecta-gov.br.

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.258
ISSN 2595-4717

Brasil. 2024b. "Entenda o projeto de Rede Privativa de Comunicação da Administração Pública Federal." Brasília: Governo Digital. Acesso em 22 de outubro de 2024. https://www.gov.br/anatel/pt-br/assuntos/noticias/entenda-o-projeto-de-rede-privativa-de-comunicacao-da-administracao-publica-federa.

Brasil. 2024c. "Infraestrutura Nacional de Dados." Brasília: Governo Digital. Acesso em 22 de outubro de 2024. https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados.

Brasil. 2024d. "O que é a diretriz Cloud First da SGD para o SISP." Brasília: Governo Digital. Acesso em 22 de outubro de 2024. https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/estrategias-e-politicas-digitais/computacao-em-nuvem/o-que-e-a-diretriz-cloud-first-da-sgd-para-o-sisp.

Brasil. 2024e. *Pesquisa sobre habilidades digitais no Brasil*. Brasília: Anatel. Acesso em 22 de outubro de 2024. https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?8-74Kn1tDR89f1Q7RjX8EYU46IzCFD26Q9Xx5QNDbqbIGuBQv-TrV78dFpuB7IKQqoNrnZCOZ3jtE5kL3VAa5556cOPI5SUdQPc8loc-tKVzQanQNRvcIh1XFEKYys8Yfr.

Brasil. 2024f. *Plano de Transformação Digital - ABIN*. Brasília: MGI. Acesso em 22 de outubro de 2024. https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/planos-de-transformacao-digital/ptds-vigentes/abin-pdx-ptd-26-mar-2024_v2-copia_tarjada.pdf.

Brasil. 2024g. "Plano Brasileiro de IA terá supercomputador e investimento de R$ 2,3 bilhões em quatro anos: IA para o bem de todos." Brasília: MCTI. Acesso em 22 de outubro de 2024. https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/noticias/2024/07/plano-brasileiro-de-ia-tera-supercomputador-e-investimento-de-r-23-bilhoes-em-quatro-anos/ia_para_o_bem_de_todos.pdf/view.

Bruneau, Thomas C. 2015. "Intelligence Reform in Brazil: A Long, DrawnOut Process," *International Journal of Intelligence and CounterIntelligence* 28 (3): 502–19. https://doi.org/10.1080/08850607.2015.1022469.

Cambricoli, Fabiana. 2020. "Nova falha do ministério da saúde expõe dados pessoais de mais de 200 milhões." *O Estado de S. Paulo*, 2 de dezembro. São Paulo, SP. Acesso em 22 de outubro de 2024. https://www.estadao.com.br/saude/nova-falha-do-ministerio-da-saude-expoe-dados-pessoais-de-mais-de-200-milhoes/.

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.258
ISSN 2595-4717

Castells, Manuel. 2009. *Communication power*. Oxford: Oxford University Press.

Castells, Manuel. 2009-2010. *The Information Age: Economy, society, and culture*. 2ª ed. Oxford: Wiley-Blackwell.

Center for Strategic and International Studies (CSIS). 2021. *Maintaining the intelligence edge: reimagining and reinventing intelligence through innovation*. Washington, D.C.: CSIS. Acesso em 22 de outubro de 2024. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210113_Intelligence_Edge.pdf.

Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (CETIC.BR). 2024a. "Portal de Dados." São Paulo: NIC.br. Acesso em 22 de outubro de 2024. https://data.cetic.br/.

Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (CETIC.BR). 2024b. *Privacidade e proteção de dados pessoais 2023: perspectivas de indivíduos, empresas e organizações públicas no Brasil*. São Paulo: NIC.br. Acesso em 22 de outubro de 2024 . https://www.cetic.br/media/docs/publicacoes/2/20240901120340/privacidade-e-protecao-de-dados-2023.pdf.

Cepik, Marco e Pedro Brancher. 2022. *Digital futures and global power: Southeast Asia and Latin America in comparative perspective*. Porto Alegre: UFRGS.

Cepik, Marco e Pedro Brancher. 2023. "Futuros digitais e poder global: Dinâmicas, desigualdades e governança," In *Soberania Popular na Era Digital*, editado por Aaron Schneider. São Paulo, SP: Fundação Perseu Abramo.

Cepik, Marco. 2005. "Regime político e sistema de inteligência no Brasil: legitimidade e efetividade como desafios institucionais," *Dados* 48 (1): 67–113. https://doi.org/10.1590/S0011-52582005000100004.

Cepik, Marco. 2021. "Intelligence and Security Services in Brazil Reappraising Institutional Flaws and Political Dynamics," *The International Journal of Intelligence, Security and Public Affairs* 23 (1): 81–102. https://doi.org/10.1080/23800992.2020.1868784.

CNN BRASIL. 2024. "Caso Siaf: governo estima desvios de R$ 3,5 milhões e 200 tentativas de pagamentos ilegais." *CNN Brasil*, São Paulo, 23 de abril. Acesso em 22 de outubro de 2024. https://www.cnnbrasil.com.br/politica/caso-siaf-governo-estima-desvios-de-r-35-milhoes-e-200-tentativas-de-pagamentos-ilegais/.

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.258
ISSN 2595-4717

Cozendey, Carlos M., Andrezza B. Barbosa e Leandro L. M. Sousa. 2021. "O projeto 'Going Digital' da OCDE: caminhos para a transformação digital no Brasil," *Revista Tempo do Mundo* 25: 155-200. https://doi.org/10.38116/rtm25art7.

Dunn, William N. 2017. *Public policy analysis: an integrated approach*. New York: Routledge.

Espanha. 2019. *Estrategia Nacional de Ciberseguridad 2019*. Madrid: Departamento de Seguridad Nacional. Acesso em 22 de outubro de 2024. https://www.dsn.gob.es/es/node/23407.

Fantástico. 2013. "Petrobras foi espionada pelos EUA, apontam documentos da NSA," *Fantástico*, Rio de Janeiro, 8 de setembro de 2013. https://g1.globo.com/fantastico/noticia/2013/09/petrobras-foi-espionada-pelos-eua-apontam-documentos-da-nsa.html.

G1. 2021. "Site da Biblioteca Nacional é retirado do ar após ataque hacker," *G1*, Rio de Janeiro, 15 de abril de 2021. Acesso em 22 de outubro de 2024. https://g1.globo.com/rj/rio-de-janeiro/noticia/2021/04/15/site-da-biblioteca-nacional-e-retirado-do-ar-apos-ataque-hacker.ghtml.

Gill, Peter. 2012. "Alguns aspectos da reforma da inteligência na América Latina," *Varia História* 28 (47): 101-120. https://doi.org/10.1590/S0104-87752012000100006.

Gonçalves, Joanisval Brito e Rodrigo Bedritichuk. 2024. "Controle parlamentar da inteligência no Brasil: análise e propostas de mudanças na CCAI," *Núcleo de Estudos e Pesquisas da Consultoria Legislativa do Senado Federal*. Texto para Discussão nº 331. Brasília: Senado Federal. Acesso em 22 de outubro de 2024. https://www12.senado.leg.br/publicacoes/estudos-legislativos/tipos-de-estudos/textos-para-discussao/td331a.

Guterman, Ofer. 2023. "Open Intelligence: A new framework for relations between intelligence organizations and the civilian sphere," *The Institute for the Research of the Methodology of Intelligence*. Acesso em 22 de outubro de 2024. https://www.intelligence-research.org.il/userfiles/banners/Ofer_Guterman_Open_intelligence.pdf.

Kollars, Nina. 2023. "Taking Non-State Actors Seriously (No, Seriously)," In *Deter, Disrupt, or Deceive: Assessing Cyber Conflict as an Intelligence Contest*, editado por Robert Chesney e Max Smeets. Washington, D.C.: Georgetown University Press.

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.258
ISSN 2595-4717

Lakatos, Eva Maria e Marina de Andrade Marconi. 2017. *Fundamentos de metodologia científica*. São Paulo: Atlas.

Lang, Volker. 2021. *Digital fluency: understanding the basics of artificial intelligence, blockchain technology, quantum computing, and their applications for digital transformation*. Berkeley, CA: Apress.

Lima, José Vinícus V., Fernanda Alencar, Cleyton Rodrigues e Wylliams Santos. 2023. "Transformação digital no setor público: resultados preliminares de um estudo terciário," In *Anais estendidos do XIX simpósio brasileiro de sistemas de informação*. Porto Alegre: Sociedade Brasileira de Computação. https://doi.org/10.5753/sbsi_estendido.2023.229395.

Mercuri, Karen T. e Rodrigo E. de Lima-Lopes. 2020. "Discurso de ódio em mídias sociais como estratégia de persuasão popular," *Trabalhos em Linguística Aplicada* 59 (2): 1216-1238. https://doi.org/10.1590/0103181376099162020072 3.

Mitkiewicz, Fernando. 2024. "Transformação digital: análise da implantação da plataforma Gov.br e da evolução da maturidade da política de governo digital no Brasil," In *Digitalização e tecnologias da informação e comunicação: oportunidades e desafios para o Brasil*, editado por Luis Claudio Kubota. Brasília: IPEA.

Organização para a Cooperação e Desenvolvimento Econômico (OCDE). 2018. *Revisão do governo digital do Brasil: rumo à transformação digital do setor público - Principais conclusões*. Brasília: OCDE. https://repositorio.enap.gov.br/handle/1/3627.

Organização para a Cooperação e Desenvolvimento Econômico (OCDE). 2020. *Latin American economic outlook 2020: digital transformation for building back better*. [S. l.]: OCDE. https://doi.org/10.1787/e6e-864fb-en.

Pereira, Caroline N. e César N. de Castro. 2022. "Expansão da produção agrícola, novas tecnologias de produção, aumento de produtividade e o desnível tecnológico no meio rural," *Instituto de Pesquisa Econômica Aplicada (IPEA)*. Texto para Discussão nº 2765. Brasília: IPEA. https://doi.org/10.38116/td2765.

Plekhanov, Dmitry, Henrik Franke e Torbjørn H. Netland. 2023. "Digital transformation: A review and research agenda," *European Management Journal* 41 (6). https://doi.org/10.1016/j.emj.2022.09.007.

Revista Brasileira de Inteligência
2024 • nº 19 • e2024.19.258
ISSN 2595-4717

Hockenhull, Jim. 2022. "How Open Source Intelligence has shaped the Russia-Ukraine war." Reino Unido, Ministério da Defesa. Acesso em 22 de outubro de 2024. https://www.gov.uk/government/speeches/how-open-source-intelligence-has-shaped-the-russia-ukraine-war.

Ribeiro, Manuella M., Javiera F. M. Macaya e Luciana P. B. Lima. 2022. "Transformação digital no governo: tendências e legados da pandemia," *Panorama Setorial da Internet* 14 (4): 1-32.

Secchi, Leonardo. 2013. *Políticas Públicas: conceitos, esquemas de análise, casos práticos*. São Paulo: Cengage Learning.

Śledziewska, Katarzyna e Renata Włoch. 2021. *The economics of digital transformation: the disruption of markets, production, consumption and work*. Abingdon, Oxon: Routledge.

Smeets, Max W. E. e Herbert Lin. 2018. "A Strategic Assessment of the U.S. Cyber Command Vision," In *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*, editado por Herbert Lin e Amy Zegart. Washington, D.C.: Brookings Institution Press, 81-104.

Special Competitive Studies Project (SCSP). 2024. "Intelligence Innovation: repositioning for future technology competition." Acesso em 22 de outubro de 2024. https://www.scsp.ai/wp-content/uploads/2024/04/Intelligence-Innovation.pdf.

Souza, Carlos Affonso de. 2020. "O que o ataque hacker ao STJ ensina sobre segurança digital," *UOL Tilt*, São Paulo, 6 de novembro de 2020. Acesso em 22 de outubro de 2024. https://www.uol.com.br/tilt/colunas/carlos-affonso-de-souza/2020/11/06/o-que-o-ataque-hacker-ao-stj-ensina-sobre-seguranca-digital.htm.

United States Studies Centre (USSC). 2023. "Submission to the 2024 Independent Intelligence Review." Acesso em 22 de outubro de 2024. https://www.ussc.edu.au/submission-to-the-2024-independent-intelligence-review.

Vial, Gregory. 2019. "Understanding Digital Transformation: A Review and a Research Agenda," *The Journal of Strategic Information Systems* 28 (2): 118-144. https://doi.org/10.1016/j.jsis.2019.01.003.

Zegart, Amy. 2022. *Spies, Lies, and Algorithms: The History and Future of American Intelligence*. Princeton, NJ: Princeton University Press.