RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano VII, v.2 2026 | submissão: 21/08/2026 | aceito: 22/08/2026 | publicação: 27/08/2026

Governança de dados, privacidade e robotic process automation: desafios estratégicos para o tratamento automatizado de dados nas organizações

Data governance, privacy, and robotic process automation: strategic challenges for automated data processing in organizations

André Mendonça Filho

RESUMO

A transformação digital tem ampliado o uso de dados como recurso estratégico para organizações públicas e privadas, ao mesmo tempo em que tecnologias de automação passaram a desempenhar papel relevante na execução de atividades operacionais. Nesse contexto, a Robotic Process Automation (RPA) destaca-se pela capacidade de automatizar tarefas repetitivas, estruturadas e baseadas em regras, proporcionando ganhos relacionados à produtividade, padronização e eficiência. Entretanto, a utilização de robôs de software em processos que envolvem dados pessoais amplia a necessidade de mecanismos de governança e proteção da privacidade. Este artigo tem como objetivo analisar a relação entre governança de dados, privacidade e RPA, enfatizando os principais desafios associados ao tratamento automatizado de dados. Realizou-se uma pesquisa bibliográfica e documental, de abordagem qualitativa e de caráter exploratório e descritivo, fundamentada em artigos científicos, legislação e documentos técnicos nacionais e internacionais. A análise demonstra que a adoção de RPA não deve ser compreendida como uma iniciativa tecnológica, mas como um processo organizacional que exige a definição de responsabilidades, o controle de acessos, a rastreabilidade, a qualidade dos dados, a avaliação de riscos e a prestação de contas. A governança de dados constitui elemento estruturante para garantir que os robôs operem dentro de parâmetros definidos e compatíveis com os princípios de proteção de dados. Conclui-se que a integração entre governança, privacidade e RPA contribui para uma automação mais segura, transparente, eficiente e alinhada às exigências regulatórias.

Palavras-chave: Governança de dados. Privacidade. Proteção de dados. Robotic Process Automation.

ABSTRACT

Digital transformation has significantly expanded the use of data as a strategic resource for public and private organizations, while automation technologies have become increasingly relevant in the execution of operational activities. In this context, Robotic Process Automation (RPA) stands out for its ability to automate repetitive, structured, and rule-based tasks, generating benefits related to productivity, standardization, and efficiency. However, the use of software robots in processes involving personal data increases the need for effective governance and privacy protection mechanisms. This article aims to analyze the relationship between data governance, privacy, and RPA, emphasizing the main challenges associated with automated data processing. Methodologically, a bibliographic and documentary study was conducted using a qualitative, exploratory, and descriptive approach, based on scientific articles, legislation, and national and international technical documents. The analysis demonstrates that RPA adoption should not be understood exclusively as a technological initiative, but as an organizational process requiring defined responsibilities, access controls, traceability, data quality, risk assessment, and accountability mechanisms. Data governance constitutes a structural element for ensuring that software robots operate within predefined parameters and in accordance with data protection principles. It is concluded that the integration of governance, privacy, and RPA contributes to safer, more transparent, efficient automation aligned with regulatory requirements.

Keywords: Data governance. Privacy. Data protection. Robotic Process Automation.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano VII, v.2 2026 | submissão: 21/08/2026 | aceito: 22/08/2026 | publicação: 27/08/2026

1 INTRODUÇÃO

A crescente digitalização das atividades organizacionais transformou os dados em um dos principais ativos estratégicos das instituições. Informações relacionadas a clientes, colaboradores, fornecedores, usuários e operações passaram a ser coletadas, armazenadas, processadas e compartilhadas em grande escala. Organizações passaram a incorporar tecnologias capazes de automatizar atividades executadas por trabalhadores humanos, buscando reduzir custos, aumentar a produtividade e aprimorar a padronização dos processos.

Entre essas tecnologias, destaca-se a Robotic Process Automation (RPA), ou Automação Robótica de Processos, caracterizada pela utilização de agentes de software capazes de executar tarefas digitais a partir de regras e fluxos estabelecidos. Ao contrário da robótica industrial tradicional, a RPA atua no ambiente digital, interagindo com sistemas, aplicações, planilhas, bancos de dados e interfaces utilizadas pelos trabalhadores. Estudos apontam que a tecnologia tem sido empregada em atividades repetitivas, estruturadas e baseadas em regras.

A expansão da RPA, contudo, produz uma consequência importante: os robôs passam a participar de operações de tratamento de dados. Um bot utilizado para cadastrar clientes, consultar documentos, gerar relatórios, atualizar registros, processar pagamentos ou transferir informações entre sistemas pode ter acesso a dados pessoais e, em determinadas situações, a dados pessoais sensíveis.

Nesse cenário, a eficiência proporcionada pela automação precisa ser acompanhada por mecanismos capazes de assegurar que o tratamento dos dados ocorra de maneira legítima, segura, necessária e compatível com as finalidades estabelecidas pela organização. No Brasil, essa preocupação encontra respaldo na Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD), que estabelece regras e princípios aplicáveis ao tratamento de dados pessoais.

A LGPD estabelece princípios como finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas. Tais princípios possuem implicações diretas sobre projetos de automação, uma vez que o uso de robôs não elimina as responsabilidades da organização em relação aos dados processados.

Nesse sentido, a governança de dados assume papel fundamental. Ela estabelece estruturas, responsabilidades, políticas e controles destinados a garantir que os dados sejam administrados de maneira adequada ao longo de seu ciclo de vida. Quando associada à RPA, a governança permite determinar quais informações podem ser acessadas pelos robôs, quais atividades podem ser executadas, quais registros devem ser mantidos e quais mecanismos devem ser utilizados para identificar e corrigir desvios.

O National Institute of Standards and Technology (NIST) destaca que a gestão da privacidade deve

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 21/08/2026 | aceito: 22/08/2026 | publicação: 27/08/2026

ser integrada à gestão de riscos organizacionais, possibilitando que as instituições identifiquem, avaliem e tratem impactos relacionados ao processamento de dados pessoais. O órgão também vem desenvolvendo uma abordagem específica de integração entre governança e gestão de dados e privacidade.

Diante desse contexto, este artigo tem como objetivo analisar a relação entre governança de dados, privacidade e Robotic Process Automation, discutindo de que maneira mecanismos de governança podem contribuir para a utilização segura e responsável da automação de processos.

A questão norteadora da pesquisa é: de que maneira a governança de dados e os mecanismos de proteção da privacidade podem contribuir para a implementação segura de soluções de RPA nas organizações?

2 METODOLOGIA

O presente estudo caracteriza-se como uma pesquisa bibliográfica e documental, de abordagem qualitativa e natureza exploratória e descritiva.

A pesquisa bibliográfica foi desenvolvida a partir da análise de artigos científicos, estudos de revisão da literatura e trabalhos acadêmicos relacionados à Robotic Process Automation, governança de dados, proteção de dados, privacidade e gestão de riscos. Foram considerados trabalhos que contribuíssem para a compreensão conceitual e organizacional da RPA, bem como estudos voltados aos desafios de governança e segurança associados à automação.

Entre as referências utilizadas destaca-se o estudo de Syed et al. (2020), que realizou uma revisão estruturada da literatura sobre RPA e identificou diferentes temas e desafios relacionados à tecnologia, incluindo questões referentes à implementação, operação e desenvolvimento de robôs.

Também foram considerados estudos voltados à governança de RPA. Kedziora e Penttinen (2021), por exemplo, analisaram a experiência de governança de RPA no contexto do Nordea Bank, evidenciando a necessidade de tratar aspectos relacionados ao desenvolvimento, manutenção, infraestrutura e governança das soluções automatizadas.

A pesquisa documental contemplou a Lei nº 13.709/2018, os dispositivos relacionados aos princípios de proteção de dados, direitos dos titulares, responsabilidades dos agentes de tratamento, registro das operações e segurança.

Também foram analisados documentos do NIST relacionados ao Privacy Framework e à integração entre governança e gestão de dados. O Privacy Framework propõe uma abordagem baseada em riscos para que organizações identifiquem e administrem riscos de privacidade, sendo aplicável a diferentes setores e tecnologias.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.
Ano VII, v.2 2026 | submissão: 21/08/2026 | aceito: 22/08/2026 | publicação: 27/08/2026

A análise do material selecionado foi realizada de maneira interpretativa, buscando identificar convergências entre os conceitos de governança de dados, privacidade e automação de processos. O procedimento permitiu organizar a discussão em três eixos principais: governança e qualidade dos dados; privacidade e proteção de dados pessoais; e governança do ciclo de vida das soluções de RPA.

3 REFERENCIAL TEÓRICO

3.1 Governança de dados no contexto organizacional

A governança de dados pode ser compreendida como o conjunto de estruturas, políticas, processos, responsabilidades e mecanismos de controle utilizados para assegurar que os dados sejam administrados de forma adequada aos objetivos institucionais.

Em ambientes organizacionais caracterizados pela elevada produção e circulação de informações, a ausência de governança pode produzir problemas relacionados à duplicidade de registros, inconsistência, baixa qualidade, ausência de rastreabilidade, acessos indevidos e utilização inadequada das informações.

A governança, portanto, não se limita à definição de normas técnicas. Ela envolve também a determinação de responsabilidades e a criação de mecanismos capazes de garantir que as decisões relacionadas aos dados sejam executadas de maneira consistente.

Essa perspectiva torna-se importante quando os dados são utilizados por sistemas automatizados. Um robô de software depende da qualidade das informações disponíveis para realizar as tarefas para as quais foi programado. Caso a base de dados contenha informações incompletas, incorretas ou desatualizadas, o processo automatizado poderá reproduzir e ampliar esses problemas.

A governança atua, nesse sentido, como uma camada de controle sobre o ciclo de vida dos dados. Ela pode estabelecer critérios de classificação, níveis de acesso, políticas de retenção, padrões de qualidade, mecanismos de auditoria e responsabilidades dos diferentes atores envolvidos no tratamento das informações.

O NIST reconhece a governança de dados como elemento relevante para organizações que buscam obter benefícios dos dados enquanto administram riscos relacionados à privacidade. A iniciativa de desenvolvimento do Data Governance and Management Profile procura aproximar práticas de governança de dados dos mecanismos de gestão de riscos de privacidade.

Assim, a governança de dados deve ser entendida como infraestrutura organizacional necessária para transformar dados em ativos confiáveis e controláveis em ambientes caracterizados pela automação crescente.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.
Ano VII, v.2 2026 | submissão: 21/08/2026 | aceito: 22/08/2026 | publicação: 27/08/2026

3.2 Privacidade e proteção de dados pessoais

A privacidade adquiriu importância estratégica diante da expansão das tecnologias digitais e do aumento da capacidade das organizações de coletar, processar, combinar e armazenar grandes volumes de informações.

No Brasil, a LGPD estabelece um marco normativo específico para o tratamento de dados pessoais. A legislação tem como objetivo proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural (Ferreira, 2025).

A legislação define dado pessoal como informação relacionada à pessoa natural identificada ou identificável e estabelece diferentes categorias e responsabilidades relacionadas ao tratamento dessas informações. Entre os agentes envolvidos estão o controlador, responsável pelas decisões referentes ao tratamento, e o operador, que realiza o tratamento em nome do controlador.

Um aspecto relevante para ambientes automatizados é o princípio da necessidade. Segundo esse princípio, o tratamento deve estar limitado ao mínimo necessário para a realização das finalidades estabelecidas.

Aplicado à RPA, esse princípio significa que um robô não deveria receber acesso indiscriminado a todas as informações disponíveis em um sistema porque possui capacidade para acessá-las. O acesso deve ser compatível com a atividade que o robô precisa executar. A transparência também assume relevância. As organizações devem ser capazes de compreender e demonstrar como os dados são tratados, quais agentes participam do processo e quais finalidades justificam o tratamento.

Outro elemento importante é a responsabilização. A LGPD determina que controladores e operadores mantenham registros das operações de tratamento e estabelece mecanismos relacionados à segurança e à prestação de contas.

Dessa maneira, privacidade não deve ser considerada uma etapa posterior à implementação tecnológica. Ela precisa ser incorporada desde a concepção do processo automatizado, considerando os dados utilizados, as finalidades do tratamento, os acessos concedidos e os riscos decorrentes da automação.

3.3 Robotic Process Automation

A Robotic Process Automation consiste na utilização de agentes de software para executar tarefas digitais de maneira automatizada, seguindo regras definidas. Os robôs podem interagir com interfaces, sistemas empresariais, planilhas, bancos de dados e diferentes aplicações, reproduzindo determinadas ações executadas por trabalhadores humanos.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.
Ano VII, v.2 2026 | submissão: 21/08/2026 | aceito: 22/08/2026 | publicação: 27/08/2026

Syed et al. (2020) identificam a RPA como uma tecnologia voltada à automação de tarefas e processos, destacando que os bots funcionam como agentes de software capazes de interagir com sistemas e reproduzir ações humanas. O estudo também evidencia que a área apresentou rápida adoção prática, embora tenha existido uma lacuna significativa na literatura científica.

A RPA apresenta aplicações relevantes em processos repetitivos, estruturados e baseados em regras. Aguirre e Rodriguez (2017), em estudo de caso, destacaram benefícios relacionados à produtividade e à automação de processos empresariais.

Entre os benefícios associados à RPA encontram-se:

- redução de tarefas manuais repetitivas;
- aumento da velocidade de execução;
- padronização de atividades;
- redução de determinados erros operacionais;
- disponibilidade contínua dos processos automatizados;
- possibilidade de integração entre sistemas;
- redução do tempo empregado em atividades administrativas.

Entretanto, a automação não elimina os riscos existentes no processo. Em determinadas circunstâncias, ela pode ampliá-los. Um erro humano isolado pode afetar uma operação; um erro incorporado a um robô pode ser reproduzido centenas ou milhares de vezes. Essa característica torna a governança relevante. A implantação de RPA deve contemplar seu monitoramento, manutenção, atualização, controle de acesso, documentação e eventual desativação.

3.4 Governança de RPA

A governança de RPA corresponde ao conjunto de mecanismos utilizados para orientar, controlar e supervisionar o desenvolvimento e a operação dos robôs de software.

O crescimento da utilização da RPA tem demonstrado que a criação de bots não pode ocorrer de forma descentralizada e sem critérios institucionais. A ausência de governança pode provocar duplicidade de automações, dificuldade de manutenção, acessos inadequados, ausência de documentação, dependência excessiva de indivíduos e dificuldades de auditoria.

Kedziora e Penttinen (2021), ao estudarem a governança da RPA no Nordea Bank, identificaram questões relacionadas ao desenvolvimento e manutenção dos robôs, à infraestrutura e à própria estrutura de governança. O estudo demonstra que a expansão da automação demanda mecanismos organizacionais capazes de acompanhar o ciclo de vida das soluções.

Estudos mais recentes reforçam essa perspectiva. Uma revisão sobre governança de RPA publicada

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.
Ano VII, v.2 2026 | submissão: 21/08/2026 | aceito: 22/08/2026 | publicação: 27/08/2026

em 2026 identifica como temas centrais da área os modelos de governança, gestão de mudanças organizacionais, gestão de riscos, definição de responsabilidades, regulamentação e conformidade, auditoria e controles, ciclo de desenvolvimento e segurança e privacidade.

Dessa forma, a governança de RPA deve abranger pelo menos cinco dimensões:

1. **Governança estratégica**, relacionada à definição de objetivos e prioridades de automação;
2. **Governança operacional**, voltada à execução, monitoramento e manutenção dos bots;
3. **Governança tecnológica**, relacionada à infraestrutura, integração e segurança;
4. **Governança de dados**, responsável pelos dados acessados e processados pelos robôs;
5. **Governança de privacidade e conformidade**, destinada a garantir aderência às normas e aos direitos dos titulares.

3.5 RPA e privacidade de dados

A relação entre RPA e privacidade torna-se evidente quando os robôs processam dados pessoais. Um bot pode, por exemplo, coletar informações de formulários, consultar cadastros, transferir dados entre sistemas, gerar documentos, atualizar registros ou encaminhar informações para outros setores. Cada uma dessas operações pode constituir tratamento de dados pessoais quando envolver informações relacionadas a pessoas identificadas ou identificáveis.

A principal questão não consiste, portanto, em saber se o robô é capaz de acessar determinado dado, mas se ele deve acessá-lo. Essa distinção conduz aos princípios de finalidade, adequação e necessidade estabelecidos pela LGPD. A automação deve ser construída para realizar uma finalidade específica e utilizar as informações necessárias para alcançar essa finalidade.

Outro aspecto importante refere-se ao controle de credenciais. Bots necessitam de contas de acesso para interagir com sistemas corporativos. A utilização inadequada dessas credenciais pode gerar riscos relevantes, quando vários robôs utilizam contas compartilhadas ou quando não existem mecanismos de registro das ações realizadas (Ferreira, 2025).

Por essa razão, recomenda-se que cada automação tenha identidade própria, permissões compatíveis com sua finalidade e mecanismos de registro das atividades realizadas.

A rastreabilidade também é fundamental. A organização deve conseguir identificar quando o bot executou determinada operação, quais dados foram utilizados, quais sistemas foram acessados e qual resultado foi produzido.

Nesse sentido, a governança permite transformar a automação em um processo auditável, reduzindo a possibilidade de que atividades automatizadas ocorram de maneira invisível para os responsáveis pela proteção dos dados.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.
Ano VII, v.2 2026 | submissão: 21/08/2026 | aceito: 22/08/2026 | publicação: 27/08/2026

3.6 Governança, segurança e gestão de riscos

Privacidade e segurança estão relacionadas, mas não são conceitos idênticos. O NIST destaca que a gestão de riscos de segurança contribui para a gestão de riscos de privacidade, mas não é suficiente para tratar todos os riscos relacionados à privacidade.

Essa distinção é importante no contexto da RPA. Um ambiente pode possuir mecanismos adequados de segurança contra acessos não autorizados e, ainda assim, utilizar dados pessoais de maneira excessiva ou incompatível com sua finalidade.

Por exemplo, um bot pode estar protegido contra invasões, mas ter sido configurado para copiar informações pessoais desnecessárias para a execução da tarefa. Nesse caso, existe uma questão de privacidade mesmo que não tenha ocorrido qualquer incidente de segurança.

O gerenciamento de riscos de RPA deve considerar tanto ameaças técnicas quanto riscos relacionados ao próprio desenho do tratamento de dados. Entre os principais riscos estão:

- acesso excessivo a dados pessoais;
- utilização de credenciais inadequadas;
- ausência de segregação de funções;
- compartilhamento indevido de informações;
- armazenamento de dados por período superior ao necessário;
- reprodução automatizada de informações incorretas;
- falhas na atualização dos bots;
- ausência de registros de auditoria;
- dificuldade de identificar responsabilidades;
- alteração de processos sem avaliação prévia de impacto.

A LGPD também prevê a possibilidade de elaboração de relatório de impacto à proteção de dados pessoais em determinadas situações e estabelece que o operador deve realizar o tratamento conforme as instruções fornecidas pelo controlador. Assim, projetos de RPA que envolvam dados pessoais devem incorporar avaliações de risco desde sua concepção.

3.7 Privacidade desde a concepção e ciclo de vida da automação

A proteção da privacidade deve estar presente desde as etapas iniciais do desenvolvimento de uma solução de RPA. Isso significa que os requisitos de proteção de dados devem ser considerados antes da implementação do bot. O ciclo de vida de um bot pode ser dividido em diferentes fases: identificação do processo, avaliação de viabilidade, desenho da automação, desenvolvimento, testes,

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 21/08/2026 | aceito: 22/08/2026 | publicação: 27/08/2026

implantação, monitoramento, manutenção e desativação.

Em cada uma dessas etapas existem oportunidades para inserir controles de privacidade.

Durante a seleção do processo, por exemplo, deve-se identificar quais dados serão tratados e avaliar se a automação é compatível com a finalidade pretendida. Na fase de desenvolvimento, devem ser definidos os acessos necessários. Durante os testes, devem ser utilizados mecanismos que evitem exposição desnecessária de dados reais.

Na implantação, devem ser estabelecidos mecanismos de monitoramento e registro. Durante a operação, alterações no processo ou na finalidade do tratamento devem ser avaliadas antes de modificarem o comportamento do robô.

Por fim, quando o bot deixa de ser utilizado, suas credenciais devem ser revogadas e os dados e registros relacionados devem ser tratados conforme as políticas de retenção e as exigências legais aplicáveis. A abordagem do NIST é compatível com essa perspectiva ao tratar a privacidade como atividade contínua de gestão de riscos e não como mecanismo isolado.

4 DISCUSSÃO

A análise da literatura evidencia que a relação entre governança de dados, privacidade e RPA é complementar. A RPA oferece capacidade operacional para automatizar processos; a governança fornece mecanismos de organização e controle; e a proteção da privacidade estabelece limites e responsabilidades para o tratamento de dados pessoais.

A adoção isolada da RPA pode produzir ganhos de eficiência, mas não garante um tratamento adequado das informações. Do mesmo modo, políticas de governança que não considerem as características específicas da automação podem deixar lacunas de controle.

Um dos principais desafios está na velocidade de expansão das automações. A facilidade relativa de criação de determinados bots pode estimular iniciativas descentralizadas, nas quais diferentes setores desenvolvem automações sem uma arquitetura comum de governança.

Nesse cenário, torna-se importante estabelecer um inventário de automações, contendo informações como finalidade do bot, responsável pelo processo, sistemas acessados, categorias de dados tratados, permissões concedidas, frequência de execução e controles aplicáveis.

Outro ponto relevante é a segregação de responsabilidades. O profissional responsável pela criação do robô não deve ser a única pessoa responsável pela aprovação e operação da automação. A separação de funções contribui para reduzir riscos e ampliar a capacidade de auditoria.

A qualidade dos dados também merece atenção. A automação reproduz regras, mas não possui capacidade de avaliar se as informações recebidas são adequadas. Problemas de qualidade presentes

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 21/08/2026 | aceito: 22/08/2026 | publicação: 27/08/2026

nas bases utilizadas podem ser amplificados pelo processamento automatizado (Ferreira, 2025).

A literatura contemporânea sobre governança de RPA aponta para a necessidade de estruturas mais abrangentes, envolvendo governança, gestão de riscos, conformidade, auditoria, segurança, privacidade e ciclo de vida dos robôs.

Outro aspecto importante é que a automação pode contribuir para a governança. Bots bem projetados podem produzir registros padronizados, executar controles de maneira consistente e reduzir determinadas atividades manuais suscetíveis a erros.

Portanto, RPA quando governada, pode constituir instrumento para fortalecer controles internos, padronizar processos e aumentar a rastreabilidade das operações. A questão central está, portanto, no desenho institucional da automação. O benefício tecnológico depende da existência de regras capazes de orientar seu desenvolvimento e operação.

CONCLUSÃO

A transformação digital tem ampliado a utilização de dados e a adoção de tecnologias de automação, tornando necessária uma abordagem integrada entre eficiência operacional, governança e proteção da privacidade.

A análise desenvolvida neste artigo demonstra que a Robotic Process Automation apresenta potencial significativo para automatizar tarefas repetitivas, padronizar atividades e aumentar a eficiência organizacional. Entretanto, quando os processos automatizados envolvem dados pessoais, a implantação de RPA passa a apresentar implicações relacionadas à privacidade, segurança, conformidade e responsabilização.

Nesse contexto, a governança de dados constitui elemento fundamental para estabelecer regras e responsabilidades sobre o acesso, utilização, qualidade, armazenamento e compartilhamento das informações processadas pelos robôs.

A LGPD reforça essa necessidade ao estabelecer princípios como finalidade, adequação, necessidade, transparência, segurança, prevenção e responsabilização. Esses princípios devem ser incorporados ao planejamento e à operação das soluções automatizadas, evitando que a capacidade técnica de acesso a informações seja confundida com autorização para utilizá-las.

Conclui-se que uma estratégia adequada de RPA deve contemplar governança durante todo o ciclo de vida do robô, desde a seleção do processo até sua desativação. Inventário de automações, controle de credenciais, segregação de funções, rastreabilidade, monitoramento, avaliação de riscos, qualidade dos dados e revisão periódica dos processos são mecanismos essenciais para uma automação responsável.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 21/08/2026 | aceito: 22/08/2026 | publicação: 27/08/2026

A integração entre governança de dados e RPA também permite que a automação seja utilizada como instrumento de fortalecimento dos controles internos, desde que sua implementação seja acompanhada por estruturas adequadas de supervisão.

Portanto, a principal conclusão deste estudo é que a automação de processos não deve ser dissociada da governança dos dados que sustentam esses processos. Quanto maior a participação dos robôs no tratamento de informações, maior a necessidade de mecanismos capazes de garantir que suas ações sejam legítimas, necessárias, rastreáveis e compatíveis com os direitos dos titulares.

REFERÊNCIAS

AGUIRRE, Santiago; RODRÍGUEZ, Alejandro. Automation of a business process using robotic process automation (RPA): a case study. In: FIGUEROA-GARCÍA, Juan Carlos; LÓPEZ-SANTANA, Eduardo; VILLA-RAMÍREZ, José Luis; FERRO-ESCOBAR, Roberto (eds.). *Applied Computer Sciences in Engineering*. Cham: Springer, 2017. p. 65-71. DOI: 10.1007/978-3-319-66963-2_7.

BOECKL, Katie; LEFKOVITZ, Naomi. *NIST Privacy Framework: a tool for improving privacy through enterprise risk management, version 1.0*. Gaithersburg: National Institute of Standards and Technology, 2020. DOI: 10.6028/NIST.CSWP.01162020.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018.

FERREIRA, Jorge Siqueira de Rezende. A Ousadia de um Empreendedorismo Intrépido com a Evolução da Internet de Fibra e as Mudanças Positivas na Sociedade: The Boldness of Fearless Entrepreneurship with the Evolution of Fiber Internet and Positive Changes in Society. RCMOS - Revista Científica Multidisciplinar O Saber, Brasil, v. 1, n. 1, 2025. DOI: 10.51473/rcmos.v1i1.2025.887.

KEDZIORA, Damian; PENTTINEN, Esko. Governance models for robotic process automation: the case of Nordea Bank. *Information Systems Management*, 2021. DOI: 10.1177/2043886920937022.

KOKINA, Julia; BRADFORD, Marianne. Robotic process automation governance in accounting information systems research: a multivocal literature review and future research agenda. *Journal of Information Systems*, v. 40, n. 1, p. 125, 2026. DOI: 10.2308/ISYS-2024-061.

PLATTFAUT, Ralf; BORGHOFF, Vincent. Robotic process automation: a literature-based research agenda. *Journal of Information Systems*, v. 36, n. 2, p. 173-191, 2022. DOI: 10.2308/ISYS-2020-033.

SYED, Rehan et al. Robotic process automation: contemporary themes and challenges. *Computers in Industry*, v. 115, 103162, 2020. DOI: 10.1016/j.compind.2019.103162.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). *Privacy Framework*. Gaithersburg: NIST, 2020.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). *Data Governance and Management Profile*. Gaithersburg: NIST, 2024-2026.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.