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

Year VII, vol. 2, 2026 | submitted: 08/21/2026 | accepted: 08/22/2026 | published: 08/27/2026

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

André Mendonça Filho

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.

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.

This is an open-access article published under the Creative Commons Attribution license, permitting use, distribution, and reproduction in any medium without restriction, provided the original work is properly cited.

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

Year VII, vol. 2, 2026 | submitted: 08/21/2026 | accepted: 08/22/2026 | published: 08/27/2026

1 INTRODUCTION

The increasing digitalization of organizational activities has transformed data into one of the main strategic assets of institutions. Information relating to customers, employees, suppliers, users, and operations is now collected, stored, processed, and shared on a large scale. Organizations have begun incorporating technologies capable of automating activities previously performed by human workers, seeking to reduce costs, increase productivity, and improve process standardization.

Among these technologies, Robotic Process Automation (RPA) stands out. It involves the use of software agents capable of performing digital tasks according to established rules and workflows. Unlike traditional industrial robotics, RPA operates in digital environments, interacting with systems, applications, spreadsheets, databases, and interfaces used by workers. Studies indicate that this technology has been employed for repetitive, structured, and rule-based activities.

The expansion of RPA, however, has an important consequence: robots become involved in data processing operations. A bot used to register customers, consult documents, generate reports, update records, process payments, or transfer information between systems may have access to personal data and, in certain situations, sensitive personal data.

In this scenario, the efficiency provided by automation must be accompanied by mechanisms ensuring that data processing is lawful, secure, necessary, and compatible with the purposes established by the organization. In Brazil, this concern is supported by Law No. 13,709/2018, the General Personal Data Protection Law (LGPD), which establishes rules and principles applicable to personal data processing.

The LGPD establishes principles such as purpose limitation, adequacy, necessity, free access, data quality, transparency, security, prevention, non-discrimination, accountability, and responsibility. These principles have direct implications for automation projects, since the use of robots does not eliminate organizational responsibility for processed data.

In this regard, data governance plays a fundamental role. It establishes structures, responsibilities, policies, and controls to ensure that data are properly managed throughout their life cycle. When associated with RPA, governance makes it possible to determine what information robots may access, what activities they may perform, what records must be maintained, and what mechanisms should be used to identify and correct deviations.

The National Institute of Standards and Technology (NIST) emphasizes that privacy management must

This is an open-access article published under the Creative Commons Attribution license, permitting use, distribution, and reproduction in any medium without restriction, provided the original work is properly cited.

Year VII, vol. 2, 2026 | submitted: 08/21/2026 | accepted: 08/22/2026 | published: 08/27/2026

be integrated into organizational risk management, enabling institutions to identify, assess, and address impacts related to personal data processing. The agency has also been developing a specific approach to integrating data governance and management with privacy.

Against this background, this article aims to analyze the relationship between data governance, privacy, and Robotic Process Automation, discussing how governance mechanisms can contribute to the safe and responsible use of process automation.

The guiding research question is: how can data governance and privacy protection mechanisms contribute to the secure implementation of RPA solutions in organizations?

2 METHODOLOGY

This study is characterized as bibliographic and documentary research, using a qualitative approach and an exploratory and descriptive design.

The literature review was conducted through an analysis of scientific articles, literature reviews, and academic studies related to Robotic Process Automation, data governance, data protection, privacy, and risk management. Works contributing to the conceptual and organizational understanding of RPA were considered, along with studies addressing governance and security challenges associated with automation.

Among the references used is the study by Syed et al. (2020), which conducted a structured literature review on RPA and identified various themes and challenges related to the technology, including robot implementation, operation, and development.

Studies focusing on RPA governance were also considered. Kedziora and Penttinen (2021), for example, analyzed the experience of RPA governance at Nordea Bank, highlighting the need to address issues relating to the development, maintenance, infrastructure, and governance of automated solutions.

The documentary research covered Law No. 13,709/2018, including provisions on data protection principles, data subjects’ rights, the responsibilities of processing agents, records of processing operations, and security.

NIST documents relating to the Privacy Framework and the integration of governance and data management were also examined. The Privacy Framework proposes a risk-based approach through which organizations identify and manage privacy risks, applicable across different sectors and technologies.

This is an open-access article published under the Creative Commons Attribution license, permitting use, distribution, and reproduction in any medium without restriction, provided the original work is properly cited.

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

Year VII, vol. 2, 2026 | submitted: 08/21/2026 | accepted: 08/22/2026 | published: 08/27/2026

The selected material was analyzed interpretively, seeking to identify convergences among the concepts of data governance, privacy, and process automation. This procedure made it possible to organize the discussion around three main themes: data governance and quality; privacy and personal data protection; and governance of the RPA solution life cycle.

3 THEORETICAL FRAMEWORK

3.1 Data governance in the organizational context

Data governance can be understood as the set of structures, policies, processes, responsibilities, and control mechanisms used to ensure that data are managed in accordance with institutional objectives.

In organizational environments characterized by high volumes of information production and circulation, the absence of governance can lead to duplicate records, inconsistencies, poor quality, lack of traceability, unauthorized access, and improper use of information.

Governance, therefore, is not limited to defining technical standards. It also involves assigning responsibilities and creating mechanisms to ensure that decisions concerning data are implemented consistently.

This perspective becomes important when data are used by automated systems. A software robot depends on the quality of available information to perform the tasks for which it was programmed. If a database contains incomplete, incorrect, or outdated information, the automated process may reproduce and amplify those problems.

In this sense, governance functions as a control layer over the data life cycle. It may establish classification criteria, access levels, retention policies, quality standards, auditing mechanisms, and responsibilities for the different actors involved in processing information.

NIST recognizes data governance as a relevant element for organizations seeking to benefit from data while managing privacy-related risks. The Data Governance and Management Profile initiative seeks to bring data governance practices closer to privacy risk management mechanisms.

Thus, data governance should be understood as an organizational infrastructure necessary to transform data into reliable and controllable assets in environments characterized by increasing automation.

This is an open-access article published under the Creative Commons Attribution license, permitting use, distribution, and reproduction in any medium without restriction, provided the original work is properly cited.

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

Year VII, vol. 2, 2026 | submitted: 08/21/2026 | accepted: 08/22/2026 | published: 08/27/2026

3.2 Privacy and personal data protection

Privacy has acquired strategic importance with the expansion of digital technologies and the growing capacity of organizations to collect, process, combine, and store large volumes of information.

In Brazil, the LGPD establishes a specific legal framework for personal data processing. The legislation aims to protect the fundamental rights to freedom and privacy and the free development of the personality of natural persons (Ferreira, 2025).

The legislation defines personal data as information relating to an identified or identifiable natural person and establishes different categories and responsibilities associated with processing such information. The agents involved include the controller, responsible for decisions regarding processing, and the processor, which processes data on behalf of the controller.

An important aspect for automated environments is the principle of necessity. Under this principle, processing must be limited to the minimum necessary to achieve the established purposes.

Applied to RPA, this principle means that a robot should not be given unrestricted access to all information available in a system simply because it has the technical capacity to access it. Access must be compatible with the activity the robot needs to perform. Transparency is also important. Organizations must be able to understand and demonstrate how data are processed, which agents participate in the process, and which purposes justify processing.

Another important element is accountability. The LGPD requires controllers and processors to maintain records of processing operations and establishes mechanisms relating to security and accountability.

Accordingly, privacy should not be considered a step following technological implementation. It must be incorporated from the design of the automated process, taking into account the data used, the purposes of processing, the access granted, and the risks arising from automation.

3.3 Robotic Process Automation

Robotic Process Automation involves the use of software agents to perform digital tasks automatically according to defined rules. Robots can interact with interfaces, enterprise systems, spreadsheets, databases, and different applications, reproducing certain actions performed by human workers.

This is an open-access article published under the Creative Commons Attribution license, permitting use, distribution, and reproduction in any medium without restriction, provided the original work is properly cited.

Year VII, vol. 2, 2026 | submitted: 08/21/2026 | accepted: 08/22/2026 | published: 08/27/2026

Syed et al. (2020) identify RPA as a technology designed to automate tasks and processes, noting that bots function as software agents capable of interacting with systems and reproducing human actions. Their study also shows that the field experienced rapid practical adoption, although a significant gap remained in the scientific literature.

RPA has relevant applications in repetitive, structured, and rule-based processes. Aguirre and Rodríguez (2017), in a case study, highlighted benefits related to productivity and business process automation.

Benefits associated with RPA include:

• reduction of repetitive manual tasks;
• increased execution speed;
• standardization of activities;
• reduction of certain operational errors;
• continuous availability of automated processes;
• possibility of integration between systems;
• reduction of time spent on administrative activities.

However, automation does not eliminate existing process risks. Under certain circumstances, it may increase them. An isolated human error may affect one operation; an error embedded in a robot may be reproduced hundreds or thousands of times. This characteristic makes governance relevant. RPA implementation must include monitoring, maintenance, updating, access control, documentation, and eventual decommissioning.

3.4 RPA governance

RPA governance comprises the mechanisms used to guide, control, and supervise the development and operation of software robots.

The growth in RPA use has shown that bots cannot be created in a decentralized manner without institutional criteria. A lack of governance may result in duplicate automations, maintenance difficulties, inappropriate access, missing documentation, excessive dependence on individuals, and auditing difficulties.

Kedziora and Penttinen (2021), studying RPA governance at Nordea Bank, identified issues related to robot development and maintenance, infrastructure, and governance structures themselves. The study demonstrates that the expansion of automation requires organizational mechanisms capable of overseeing the solution life cycle.

More recent studies reinforce this perspective. A review of RPA governance published

This is an open-access article published under the Creative Commons Attribution license, permitting use, distribution, and reproduction in any medium without restriction, provided the original work is properly cited.

Year VII, vol. 2, 2026 | submitted: 08/21/2026 | accepted: 08/22/2026 | published: 08/27/2026

in 2026 identifies governance models, organizational change management, risk management, assignment of responsibilities, regulation and compliance, auditing and controls, the development life cycle, and security and privacy as central themes in the field.

Thus, RPA governance should encompass at least five dimensions:

1. Strategic governance, related to the definition of automation objectives and priorities;
2. Operational governance, focused on the execution, monitoring, and maintenance of bots;
3. Technological governance, related to infrastructure, integration, and security;
4. Data governance, responsible for data accessed and processed by robots;
5. Privacy and compliance governance, intended to ensure adherence to regulations and data subjects' rights.

3.5 RPA and data privacy

The relationship between RPA and privacy becomes evident when robots process personal data. A bot may, for example, collect information from forms, consult records, transfer data between systems, generate documents, update records, or forward information to other departments. Each of these operations may constitute personal data processing when it involves information relating to identified or identifiable persons.

The main question, therefore, is not whether the robot is capable of accessing certain data, but whether it should access them. This distinction leads to the principles of purpose, adequacy, and necessity established by the LGPD. Automation must be designed to achieve a specific purpose and use the information necessary to achieve it.

Another important aspect concerns credential control. Bots require access accounts to interact with corporate systems. Improper use of these credentials may create significant risks when multiple robots use shared accounts or when there are no mechanisms for recording the actions performed (Ferreira, 2025).

For this reason, it is recommended that each automation have its own identity, permissions consistent with its purpose, and mechanisms for recording the activities performed.

Traceability is also fundamental. The organization must be able to identify when a bot performed a given operation, what data were used, which systems were accessed, and what result was produced.

In this sense, governance makes automation an auditable process, reducing the possibility that automated activities occur invisibly to those responsible for data protection.

This is an open-access article published under the Creative Commons Attribution license, permitting use, distribution, and reproduction in any medium without restriction, provided the original work is properly cited.

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

Year VII, vol. 2, 2026 | submitted: 08/21/2026 | accepted: 08/22/2026 | published: 08/27/2026

3.6 Governance, security, and risk management

Privacy and security are related but are not identical concepts. NIST emphasizes that security risk management contributes to privacy risk management but is not sufficient to address all privacy-related risks.

This distinction is important in the RPA context. An environment may have adequate security mechanisms against unauthorized access and still use personal data excessively or in a manner incompatible with their intended purpose.

For example, a bot may be protected against intrusions but configured to copy personal information that is unnecessary for performing its task. In that case, a privacy issue exists even if no security incident has occurred.

RPA risk management must consider both technical threats and risks associated with the design of data processing itself. The main risks include:

• excessive access to personal data;
• use of inappropriate credentials;
• lack of segregation of duties;
• improper sharing of information;
• retention of data longer than necessary;
• automated reproduction of incorrect information;
• failures in updating bots;
• absence of audit logs;
• difficulty identifying responsibilities;
• changes to processes without prior impact assessment.

The LGPD also provides for the possibility of preparing a personal data protection impact assessment in certain situations and establishes that the processor must process data in accordance with instructions provided by the controller. Thus, RPA projects involving personal data must incorporate risk assessments from the design stage.

3.7 Privacy by design and the automation life cycle

Privacy protection must be present from the earliest stages of developing an RPA solution. This means that data protection requirements must be considered before implementing the bot. A bot’s life cycle can be divided into different phases: process identification, feasibility assessment, automation design, development, testing,

This is an open-access article published under the Creative Commons Attribution license, permitting use, distribution, and reproduction in any medium without restriction, provided the original work is properly cited.

Year VII, vol. 2, 2026 | submitted: 08/21/2026 | accepted: 08/22/2026 | published: 08/27/2026

deployment, monitoring, maintenance, and decommissioning.

Each of these stages offers opportunities to introduce privacy controls.

During process selection, for example, the data to be processed should be identified and the compatibility of automation with the intended purpose assessed. During development, the necessary access permissions should be defined. During testing, mechanisms should be used to avoid unnecessary exposure of real data.

At deployment, monitoring and recording mechanisms must be established. During operation, changes in the process or purpose of processing must be evaluated before they alter the robot's behavior.

Finally, when a bot is no longer used, its credentials must be revoked, and related data and records must be handled in accordance with retention policies and applicable legal requirements. NIST's approach is consistent with this perspective in treating privacy as an ongoing risk management activity rather than an isolated mechanism.

4 DISCUSSION

The literature analysis shows that the relationship among data governance, privacy, and RPA is complementary. RPA provides the operational capacity to automate processes; governance supplies organization and control mechanisms; and privacy protection establishes limits and responsibilities for personal data processing.

The isolated adoption of RPA may generate efficiency gains but does not guarantee proper handling of information. Similarly, governance policies that fail to consider the specific characteristics of automation may leave gaps in control.

One of the main challenges lies in the speed at which automations expand. The relative ease of creating certain bots may encourage decentralized initiatives in which different departments develop automations without a common governance architecture.

In this scenario, it is important to establish an automation inventory containing information such as the bot's purpose, the person responsible for the process, systems accessed, categories of data processed, permissions granted, execution frequency, and applicable controls.

Another relevant issue is the segregation of responsibilities. The professional responsible for creating the robot should not be the sole person responsible for approving and operating the automation. Separation of duties helps reduce risks and increase auditability.

Data quality also deserves attention. Automation reproduces rules but does not have the ability to assess whether the information received is appropriate. Quality problems present

This is an open-access article published under the Creative Commons Attribution license, permitting use, distribution, and reproduction in any medium without restriction, provided the original work is properly cited.

Year VII, vol. 2, 2026 | submitted: 08/21/2026 | accepted: 08/22/2026 | published: 08/27/2026

in the databases used may be amplified by automated processing (Ferreira, 2025).

Contemporary literature on RPA governance points to the need for more comprehensive structures encompassing governance, risk management, compliance, auditing, security, privacy, and the robot life cycle.

Another important aspect is that automation can contribute to governance. Well-designed bots can produce standardized records, execute controls consistently, and reduce certain error-prone manual activities.

Therefore, when properly governed, RPA can serve as an instrument to strengthen internal controls, standardize processes, and increase the traceability of operations. The central issue, therefore, lies in the institutional design of automation. Technological benefits depend on the existence of rules capable of guiding its development and operation.

CONCLUSION

Digital transformation has expanded the use of data and the adoption of automation technologies, making an integrated approach to operational efficiency, governance, and privacy protection necessary.

The analysis developed in this article demonstrates that Robotic Process Automation has significant potential to automate repetitive tasks, standardize activities, and increase organizational efficiency. However, when automated processes involve personal data, RPA implementation has implications for privacy, security, compliance, and accountability.

In this context, data governance is a fundamental element for establishing rules and responsibilities regarding access, use, quality, storage, and sharing of information processed by robots.

The LGPD reinforces this need by establishing principles such as purpose, adequacy, necessity, transparency, security, prevention, and accountability. These principles must be incorporated into the planning and operation of automated solutions, preventing technical capacity to access information from being confused with authorization to use it.

It is concluded that an appropriate RPA strategy must include governance throughout the robot life cycle, from process selection to decommissioning. An automation inventory, credential control, segregation of duties, traceability, monitoring, risk assessment, data quality, and periodic process review are essential mechanisms for responsible automation.

This is an open-access article published under the Creative Commons Attribution license, permitting use, distribution, and reproduction in any medium without restriction, provided the original work is properly cited.

Year VII, vol. 2, 2026 | submitted: 08/21/2026 | accepted: 08/22/2026 | published: 08/27/2026

The integration of data governance and RPA also allows automation to be used as a tool for strengthening internal controls, provided its implementation is accompanied by appropriate oversight structures.

Therefore, the main conclusion of this study is that process automation must not be separated from the governance of the data underpinning those processes. The greater the involvement of robots in information processing, the greater the need for mechanisms ensuring that their actions are legitimate, necessary, traceable, and compatible with data subjects' rights.

REFERENCES

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.

BRAZIL. Law No. 13,709 of August 14, 2018. General Personal Data Protection Law (LGPD). Brasília, DF: Presidency of the Republic, 2018.

FERREIRA, Jorge Siqueira de Rezende. The Boldness of Fearless Entrepreneurship with the Evolution of Fiber Internet and Positive Changes in Society. RCMOS - Revista Científica Multidisciplinar O Saber, Brazil, v. 1, no. 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, no. 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, no. 2, pp. 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.

This is an open-access article published under the Creative Commons Attribution license, permitting use, distribution, and reproduction in any medium without restriction, provided the original work is properly cited.