STUDY

Leonel Moya and Mailén García
May 2026

Negotiating Digitalised Workplaces

Rights and Obligations, Brazil

Friedrich Ebert Stiftung

Imprint

Publisher
Friedrich-Ebert-Stiftung e.V.
Godesberger Allee 149
53175 Bonn
Germany
info@fes.de

Publishing department
Division for International Cooperation |
Global and European Policy

Responsibility for content and editing
Mirko Herberg, Director, Global Trade Union Project

Contact
Blanka Balfer
blanka.balfer@fes.de

Design/Layout
pertext | corporate publishing
www.pertext.de

May 2026

ISBN 978-3-98628-880-8

Further publications of the Friedrich-Ebert-Stiftung can be found here:
↗ www.fes.de/publikationen

Friedrich Ebert Stiftung

Leonel Moya and Mailén García
May 2026

Negotiating Digitalised Workplaces

Rights and Obligations, Brazil

Contents

Foreword

Across the world, management in both the public and private sectors is deploying digital technologies with the aim of improving productivity and efficiency. Such technologies have a direct impact on working conditions and workers' rights. Jobs are being (semi-)automated, new competencies are required and work and workers are becoming quantified as their actions and non-actions are turned into data points and analysed through algorithmic systems. The negative impact of these systems on workers is well documented.

Yet anecdotal evidence from multiple countries suggests that shop stewards and Occupational Health and Safety representatives to a large degree are not discussing the use of digital technologies with management. The representatives mention that they feel they lack knowledge about the particularities of digital technologies and why they should pay careful attention to them. Many report that management never raises the issues of digitalisation with them, nor do they feel they have a sound overview of how to apply existing laws and agreements to spur these discussions.

Although some unions are successfully negotiating contract language about the digitalisation of work as evidenced by PSI's Digital Bargaining Hub, the vast majority are still not. To support unions in their negotiations with management, this series of reports brings to light what rights workers have when digital systems are deployed at work and what obligations management have in relation to the workers. The reports provide ready-to-use checklists of questions, and collective bargaining suggestions to bridge legal gaps.

The Friedrich-Ebert-Stiftung realises that technology deployment without workers involvement not only subjects workers to control but also changes the balance of power at the workplace in favour of employers. Workers may feel increasingly alienated and objectified. We have understood that an unprotected and disempowered workforce is not only less productive but tends to lose trust in the promises and institutions that are supposed to guarantee decent work and a decent live. Therefore, contributing to workers' capacity to claim their rights and negotiate working conditions in a digitalised workplace is a service to democracy and justice. This is what this project aims to achieve – by making transparent what institutional power, i.e. rights, laws and labour market agreements workers have at their disposal. We hope that the case studies presented will lead to a more thorough and strategic response by workers and organised labour in the countries studied and to more countries embarking on the path towards negotiated introduction and use of digital technologies.

We owe Christina J. Colclough, Director of The Why Not Lab, Denmark, our gratitude for providing the initial spark for this project and for being an enthusiastic and competent mentor to the case study authors. Her relentless dedication to challenge, motivate and capacity build the labour movement to build power in the digital economy is unparalleled and has been the inspiration behind many collaborative undertakings of the FES Global and national Trade Union Projects.

We thank the authors of the country studies for their professionalism and enthusiasm to explore uncharted territory, for the discoveries of potential leverage points and for their "thinking forward" to take the next steps in building workers' power.

Finally, Blanka Balfer, FES, deserves praise for being the silent backbone of this project (and so many others) that allow FES to use its global network for the benefit of the global labour movement.

May this series of reports serve as a stepping stone for deeper engagement, collective bargaining and policy-making and policy-enforcing success in the digital economy of today and tomorrow!

Mirko Herberg
Director, Global Trade Union Project
Friedrich-Ebert-Stiftung

1.
Introduction – Technology at Work Is a Labour Issue

You may already be working with digital technologies without having been asked about them. An app to clock in. Software that scores your calls. Dashboards measuring performance. GPS tracking in vehicles. AI screening job applications. Cameras in new places. These technologies are often presented as technical tools to improve efficiency or service quality. But for workers, they change how work is organised, monitored, evaluated, and controlled.

This report is designed to help workers and unions understand which laws already apply, which questions they have a right to ask based on those laws, and how to use those rights when digital technologies are introduced or used at work. It also shows how collective bargaining can be used to address gaps that existing law does not fully regulate.

Digital technologies are no longer peripheral tools in the workplace. Across the world, they increasingly sit at the centre of managerial power, shaping how work is organised, paced, evaluated and controlled. Biometric attendance systems, GPS tracking, algorithmic task allocation, AI-based recruitment tools, performance dashboards and automated decision-making systems are being rolled out across sectors with little warning and, too often, without meaningful consultation with workers or their trade unions.

For workers and union officials, this transformation raises a fundamental question: who controls technology at work, and in whose interests is it deployed? While employers routinely present digitalisation as neutral, inevitable or purely technical, workers experience it as a restructuring of power relations. Digital systems extend managerial oversight into new areas of workers' lives, intensify work, fragment tasks, obscure decision-making and deepen information asymmetries between employers and workers.

Digitalisation is also frequently used to bypass established industrial-relations practices. New technologies are introduced as matters of managerial prerogative; data are collected without transparency; and algorithmic decisions are presented as objective or unchallengeable.

This report starts from a different premise. Digitalisation does not suspend labour law, weaken fundamental rights or displace collective bargaining. On the contrary, it makes union organisation, legal knowledge and collective action more necessary than ever. Existing labour law, data-protection law, equality law and occupational safety and health frameworks continue to apply in digitalised workplaces, even if they must now be asserted and enforced under new conditions.

For unions, legal clarity is therefore not an abstract concern. It is a source of bargaining power. Knowing which rights already exist – and where they fall short – enables unions to challenge unilateral technological change, demand information and consultation, and negotiate binding protections that keep workers in control of how technology reshapes their jobs.

How to use this country report

This report is written for Brazilian workers, shop stewards, and trade unions who are confronting the growing use of digital technologies such as biometric timekeeping, platform-based management, GPS tracking, and automated productivity systems. In Brazil, digitalisation often advances faster than its regulation, even though the Constitution and labour law provide strong protections, including the fundamental right to protection against automation.

The report helps unions move from reactive enforcement to preventive engagement. It explains how Brazilian law applies to workplace surveillance, algorithmic management, and AI systems, and how these rules can be used strategically in discussions with management.

The report includes a checklist of key questions based on legal rights that workers and unions can use *before* a new technology is introduced and periodically while it is being used. These questions are intended to structure negotiations, demand information, and prevent technologies from being imposed unilaterally or expanded without consent.

The purpose of the report is practical and strategic: it aims to support workers and unions in understanding what digitalisation means for their rights, to strengthen their position in discussions with management, and to help turn abstract legal protections into concrete, enforceable workplace standards.

No legal ecosystem fully addresses the risks to workers' rights, dignity and decent work. To bridge the gaps, the

report also includes a list of potential collective bargaining topics and issues for inspiration in the negotiations with management.

Digital technologies are often introduced by management as technical upgrades, efficiency tools, or unavoidable innovations. In practice, however, they frequently reshape working conditions, intensify monitoring, redistribute power, and create new risks for workers' dignity, autonomy, health, and job security. Digitalisation is not just a technical matter though. It is a labour issue and therefore a legitimate subject for negotiation, consultation, and collective bargaining.

What this report can do for you

This report is designed to help you:

- → **Identify digital technologies** being used or proposed in your workplace, even when they are presented in vague or technical language;
- → **Understand your existing rights** under labour law, data-protection rules, occupational safety and health frameworks, anti-discrimination law, and collective agreements;
- → **Hold management accountable** to its legal obligations when introducing, using, or expanding digital systems;
- → **Prepare for negotiations** by showing how other unions and workers have addressed similar challenges;
- → **Bridge gaps in the law** through collective bargaining where legal protections are weak, unclear, or poorly enforced.

Rather than assuming that digitalisation is inevitable or incontestable, the report treats it as a process that can—and must—be shaped through collective action.

How to use this report in practice

Each section of this report serves a specific purpose and can be used independently, depending on your immediate needs.

Section 2: Examples of digital technologies used in workplaces

This section provides examples of digital technologies used in Brazil. Maybe your workplace uses a similar technology, although it might be called something different? If you are in doubt about what digital technologies are used, do a virtual walk-through of a typical working day. From the moment you enter the workplace – how do you get in? Do you use an electronic keycard? Or does a technology register your fingerprint or face? Do you then need to log on to a computer technology, use a handheld device, a mobile phone, a GPS tracker, or anything else? All of these technologies are digital, and all of them create data.

If your walk-through reveals the use of digital technologies at work, this report will be highly useful for you.

Section 3: What are your rights – and what are management's obligations?

This section begins with a graphical depiction of the legal and collective frameworks that already apply to digitalised workplaces. You can use this section to quickly identify which laws, regulations, or agreements are relevant to your situation. Find the links to the laws and agreements in the Annex.

It then moves on to describe the legal and collective frameworks that already apply to digitalised workplaces. It explains what employers are required to do—such as consult workers, assess risks, limit surveillance, or ensure fairness—and how unions can invoke these obligations in discussions, negotiations, or disputes.

Section 4: The checklists of questions you have a right to ask!

Cut out this section and carry it with you when you prepare for discussions with management around the implementation and use of digital technologies in your workplace.

The questions help ensure that your rights are respected and that employers meet their obligations.

Section 5: Filling the gaps – Bargaining topic suggestions

Even when management follows the law, the law is often not enough to address how digital systems affect every day working conditions. Many of the issues raised by AI, monitoring tools, performance dashboards, and data-driven management are only partially regulated or not regulated at all by existing legislation. This is where collective bargaining becomes important. This section provides examples of bargaining themes that unions may consider when seeking to address the gaps that current law leaves open.

For further inspiration on concrete contract language unions have successfully negotiated, see Public Service International's open database that includes almost 600 clauses related to the digitalisation of work. Find it here: https://publicservices.international/digital-bargaining-hub

When can you use the report?

You can use this report at different moments:

- → **Before a technology is introduced**, to demand information, consultation, and justification;
- → **After a technology is in place**, to assess whether management is complying with its obligations;
- → **During collective bargaining**, to propose concrete clauses that regulate digitalisation;
- → **For education and organising**, to build shared understanding and collective confidence among workers.

Digital technologies do not manage themselves. Employers make choices about how they are deployed, and those choices can be questioned, negotiated, and reshaped. This report is intended to support you in doing exactly that.

2.
Examples of Digital Technologies Used in Brazilian Workplaces

Time-tracking technologies and productivity measurement

These technologies are used to record and analyse information about how and how much people work. Their main goal is to control working hours and measure productivity more accurately. In practice, they replace administrative tasks such as recording clock-ins and clock-outs, breaks, late arrivals, overtime, absences, and leaves. This way, companies can have a more detailed record of working time and evaluate staff performance.

One example is Kairos, a system developed by the Brazilian company Dimep, which is used in both private companies and some government offices. With Kairos, workers register their hours using devices with facial recognition or digital signatures in the workplace, or through a mobile app if they work remotely. All this information is automatically sent to a digital platform, where supervisors can view it, compare data, and generate reports.

This system handles personal data, including names, faces, schedules, and locations. Although it helps organize work and reduce errors, it can also create risks: it may affect workers' privacy, autonomy, and mental health. Moreover, by allowing companies to monitor employees in real-time, it increases control and deepens the information imbalance between employers and workers.

Driver tracking and telemetry technologies

These technologies are used to track drivers' movements in real time and record their activity throughout the day. Their main purpose is to monitor location, calculate the fastest routes, estimate trip prices, and evaluate drivers' performance.

An example is Uber Brazil's geolocation system, which combines the GPS on each driver's phone with services from HERE Technologies. This company specializes in digital mapping and spatial data analysis. This combination enables the app to track vehicles' locations before, during, and after each trip, assign routes, calculate fares, measure speed, and record waiting times.

The system utilizes personal information, including locations, connection times, and distances travelled. Although it helps organize the service and improve safety for both drivers and passengers, it also introduces new and less visible forms of digital control. The data generated by the app are used to assess performance and decide incentives or route assignments, which can affect drivers' job stability.

Cybersecurity technologies that log computer activities

These tools are used to protect the computer systems of companies and public institutions. To do this, they record and analyse the digital activities that people perform at work. They monitor emails, web browsing, file access, and external device connections to prevent information leaks, fraud, or cyberattacks.

An example is Symantec Endpoint Security, a software developed by the U.S. company Broadcom Inc. This program is installed on work computers and continuously monitors all activities performed on them. With that information, the system can detect behaviours it considers risky and, in those cases, block access, limit certain functions, or send alerts to security teams. The software is used primarily in the services sector, and in the telecommunications industry.

While it improves protection against attacks and data loss, it also creates a less visible form of control over workers, since all their activities are recorded and can be evaluated. In this way, automated surveillance becomes a regular part of the digital workplace, reducing workers' autonomy and trust.

3.
What Are Your Rights – And What Are Management's Obligations?

- **Constitution of the Federative Republic of Brazil (CFRB) and the Bill on the Regulation of the Principle of Protection against Automation (BRPPA)**
  The CFRB is Brazil's supreme legal framework, in force since 1988, and sets out, among other elements, fundamental rights and labour principles. The BRPPA is a bill that aims to regulate Article 7, item 27, of the CFRB by establishing safeguards for workers affected by automation; although it has not yet entered into force.

- **Consolidation of Labour Laws (CLL)**
  The CLL is Brazil's principal labour code, which organizes and regulates employment relations, workers' rights, and labour standards throughout the country. It entered into force in 1943 and has since incorporated numerous amendments and updates.

- **Regulatory Standards of the Ministry of Labour and Employment (RS)**
  The RS are technical regulations issued by Brazil's Ministry of Labour and Employment that establish mandatory requirements for workplace health, safety, and risk prevention. They entered into force progressively beginning in 1978 and have since undergone multiple revisions and updates.

- **Law on Protection against Employment Discrimination (LPED)**
  It is Brazilian legislation that prohibits discriminatory practices in hiring, employment relations, and dismissal, and outlines the legal consequences for violations. It entered into force in 1995 and has received subsequent amendments to expand its protections.

- **General Law on the Protection of Personal Data (LPPD)**
  The LPPD regulates the processing of personal data by public and private entities and safeguards fundamental rights related to privacy, freedom, and personal development. It entered into force in August 2018.

- **Law on the Use of the Internet (LUI)**
  The LUI is Brazil's legal framework that establishes principles, rights, and responsibilities for internet use, including privacy, data protection, and the neutrality of the network. It entered into force in April 2014.

- **Bill on the Use of Artificial Intelligence (BUAI)**
  The BUAI is a legislative proposal that seeks to regulate the development and use of AI systems, establishing principles, rights, and obligations to ensure transparency, safety, and accountability. As a bill, it has not yet entered into force, since it remains under discussion in the legislative process.

- **Collective Bargaining Agreements Related to Digitalization**
  These are negotiated accords between employers and trade unions that establish rules, protections, and obligations regarding the introduction and use of digital technologies in the workplace. They have been signed from 2023 onward, with their entry into force occurring upon signature and registration in each sector.

Below, we set out the key rights you already have when management decides to introduce or use digital technology at work. We do this law by law, pointing you directly to the specific provisions you need to know. Alongside your rights, we also highlight management's legal obligations to you, including duties to consult, ensure system transparency, conduct risk assessments, and more.

Then, in the next section, we bring this together into two practical sets of questions you can use to hold management to account. The first set covers questions to ask *before* a new digital technology is introduced. The second set covers your *ongoing rights* once the technology is in use. Every question is grounded in existing laws and/or collective agreements. Where management is reluctant to engage or provide answers, we reference the exact legal provisions you can rely on.

Constitution of the Federative Republic of Brazil (CFRB) and Bill on the Regulation of the Principle of Protection against Automation (BRPPA)

The CFRB, in force since 1988, protects the labour rights of all workers in the country, in both the public and private sectors, and covers urban and rural employment. Its main goal is to ensure decent, safe, and stable work.

One of the most essential rights, especially relevant in today's digital context, is the right to protection against automation **(Art. 7, item 27 of the CFRB)**. This principle states that the introduction of new technologies in the workplace cannot threaten job stability, occupational safety, or the dignity of workers.

The Constitution stipulates that this principle must be regulated through a specific law, which has yet to be enacted. However, there is a bill (BRPPA) currently under discussion, since 2019, that proposes several concrete measures, including:

- **Union Negotiation Before Automation Layoffs (Art. 2)**. Before any dismissal due to automation, the company must negotiate with the union.
- **Impact-Mitigation Plan for New Technologies (Art. 2)**. If a company plans to introduce technologies that could replace human labour, it must present a plan to minimize negative impacts, such as offering job relocation, training programs, or reduced working hours without salary loss.
- **No Increased Workload or Wage Reduction (Art. 3)**. Automation cannot be used as an excuse to increase workloads, extend working hours, or reduce wages.
- **Special Compensation for Automation-Related Dismissals (Art. 3)**. In cases of dismissal caused by automation, the affected worker is entitled to special compensation equivalent to at least three times their highest monthly salary from the past twelve months, in addition to any other benefits established by law.

Although no specific law yet regulates the principle of protecting workers from automation, Art. 7 item 27 offers a framework for union responses to technological change. In fact, many collective bargaining agreements rely on this principle and transform it into a concrete instrument that shields workers from technological replacement.

The Superior Labour Court has affirmed that collective agreements prohibiting the replacement of workers by machines are constitutional and uphold the guarantees provided by the Constitution. This precedent reinforces the notion that, even without a specific regulation, the CFRB imposes a duty of protection, allowing workers and their organizations to invoke this right in cases of omission or violation.

The content of the collective agreements mentioned is analysed on page 16f.

- **Art. 7, item 27 of the CFRB**
  It enumerates the basic rights of urban and rural workers in full. Among them, item 27 states that it is a fundamental right of workers to be protected against automation
- **Art. 2 of the BRPPA**
  Establishes that companies implementing automation in their production chain may only dismiss workers after prior collective bargaining. It also requires measures to mitigate negative impacts, such as reassignment or retraining.
- **Art. 3 of the BRPPA**
  It sets out a series of cumulative conditions that a company must follow when implementing an automation program.

Union Relevance

Trade unions may invoke item 27 of Article 7 of the CFRB to require that any automation plans companies wish to introduce into work processes that affect employees comply with standards of dignity, stability, and workplace safety. In addition, unions should keep in mind that although the principle of protection against automation is not yet regulated, it retains legitimacy as a basis for collective bargaining.

Consolidation of Labour Laws (CLL)

The CLL, in force since 1943 but with many subsequent amendments and additions, is the set of rules that regulates labour relations in the private sector. However, it also applies to public sector workers who are not covered by special administrative regimes.

Its main goal is to ensure decent, safe, and stable working conditions for these workers, regardless of the type of job they do or where they perform it.

Although many of its provisions were written before the digital era, its principles of protection, safety, and prevention remain a valid foundation for today's challenges.

Workers should know that:

- **Equal Labour Rights in All Work Modalities (Art. 6).** They have the same rights whether they work at the company, from home, or remotely. If the conditions of an employment relationship exist, the protections are the same in all cases.

- **Digital Supervision Has Full Legal Validity (Art. 6).** The technological tools their employer uses to monitor their work have the same legal value as in-person supervision. The employment relationship and the employer's obligations remain in force even when the work is performed through digital means.

- **Telework as a Fully Protected Employment Mode (Art. 75-A – 75-F)**. Remote work (or telework using digital technologies) is a legitimate form of employment, with the same rights as in-person work. This must be clearly stated in the worker's employment contract, including the tasks, technological tools, and necessary working conditions. Any change between remote and on-site work must be mutually agreed upon. If the employer decides that the worker should return to the workplace, they must give at least 15 days' notice. The company must provide or reimburse equipment and expenses, including covering internet access costs and all expenses related to working from home. It must also offer training on preventing illnesses or accidents, and respect workers' working hours, rest periods, and right to disconnect.

- **Duty to Ensure a Safe Work Environment (Art. 157)**. The employer has the obligation to guarantee a safe work environment. They must comply with health and safety regulations, inform workers about necessary precautions, and allow workplace inspections. These obligations remain valid even when digital technologies introduce new occupational risks.

- **Internal Commission for the Prevention of Accidents and Harassment (CPAH) (Art. 163)**. Companies that have employees governed by the CLL, in some cases, must establish an Internal Commission for the Prevention of Accidents and Harassment (CPAH), which includes worker representatives. This commission identifies and prevents risks and may also assess the impact of new technologies on workers' health and safety. The obligation to create a CPAH depends on the company's risk level and number of employees. When a commission is required, the size of the workforce determines how many representatives from employees and management must form part of it.

- **Provision of Safe Work Equipment (Art. 166).** The company must provide, at no cost to the worker, all equipment and resources necessary to ensure safe working conditions. In digital environments, this includes ergonomic elements, appropriate technological tools, and remote technical support to provide workers' well-being and protection.

- **Art. 6**
  It equates work performed on-site with work carried out remotely. It also establishes that digital monitoring and surveillance tools are equivalent to in-person supervision

- **Art. 75-A – 75-F**
  It sets the conditions and rights governing telework, ensuring equal protections, contractual clarity, and employer obligations regarding equipment, safety, and scheduling.

- **Art. 157**
  It establishes that the company must guarantee a safe work environment, protecting the safety and health of its employees.

- **Art. 163**
  It states that in certain cases companies must have a internal commission dedicated to identifying and preventing risks, in which workers are represented.

- **Art. 166**
  Establishes obligations for the company regarding safe working conditions.

Union Relevance

Trade unions may invoke Article 6 of the CLL to require that digital monitoring and surveillance tools be treated in the same manner as in-person mechanisms, thereby protecting workers' integrity. They may also refer to Articles 75-A through 75-F to ensure compliance with the legal provisions governing telework. Furthermore, Articles 157, 163, and 166 provide grounds for demanding safe and healthy working conditions.

Regulatory Standards of the Ministry of Labour and Employment (RS)

The RS apply to all workplaces governed by the CLL. This includes both private sector workers and public sector employees who are not covered by special administrative statutes. They were first introduced in 1978 and have been continuously updated ever since.

The main purpose of these standards is to ensure safety, health, and well-being at work. In practice, they establish the minimum conditions that every company must meet to prevent accidents, occupational illnesses, and harm to the physical or mental integrity of workers.

The RS have adapted to the growing digitalization of workplaces and now play a crucial role, since the introduction of new technologies, machinery, or automated systems can create risks that must be properly identified, assessed, and prevented.

Workers should know that:

- **Continuous Risk Assessment (RS 1)**. A risk assessment must be carried out continuously and is mandatory for all companies. Each company must regularly review its working conditions, particularly when introducing new technologies, machinery, or processes that may create new risks or modify existing ones, including risks to the physical and/or mental health of workers. This means that every technological innovation must be accompanied by a new workplace safety assessment, with active participation from workers.
- **CPAH functions (RS 5).** The CPAH (see above) is responsible for identifying hazards, proposing solutions, and monitoring the impact of technological innovations. Worker representatives who are part of the CPAH can intervene to ensure that digital innovations do not compromise workers' health or job stability.
- **Mandatory Health Monitoring (RS 7)**. The company must permanently monitor workers' health. Each company must implement a medical control program, which should be adjusted when new risks arise from digitalization or technological changes.
- **Safe Operation of Machinery and Equipment (RS 12)**. Work involving machines and equipment must be safe. All machines must have physical protections, sensors, and emergency stop mechanisms. In addition, anyone operating them must receive proper technical training. No technology should be implemented without these basic safety guarantees.
- **Ergonomic Adaptation to Individual Needs (RS 17)**. Workplace ergonomics must be adapted to each person's characteristics. Companies must conduct ergonomic assessments of workstations and adjust them to the physical and psychological needs of their employees. This is especially important in digital or automated environments, where the way work is organized can create different health risks.

- **RS 1**
  The purpose of this Standard is to establish the general provisions, scope of application, and the terms and definitions common to the RS related to occupational health and safety, as well as the guidelines and requirements for the management of occupational risks and the implementation of prevention measures in Occupational Health and Safety (OHS).
- **RS 5**
  Establishes the parameters and requirements of the CPAH, with the objective of preventing work-related accidents and illnesses, to ensure that work is permanently compatible with the preservation of life and the promotion of workers' health.

→ **RS 7**
Establishes guidelines and requirements for the development of the Occupational Health Medical Control Program (OHMCP) within organizations, aiming to protect and preserve workers' health in relation to occupational risks, in accordance with the risk assessment defined by the organization's Risk Management Program (RMP).

→ **RS 12**
Defines technical references, fundamental principles, and protective measures to safeguard workers' health and physical integrity. It establishes minimum requirements for the prevention of work-related accidents and illnesses during the design and use phases of machines and equipment, as well as for their manufacturing, importation, commercialization, exhibition, and transfer under any title, in all economic activities.

→ **RS 17**
It aims to establish the guidelines and requirements that allow the adaptation of working conditions to the psychophysiological characteristics of workers, to ensure comfort, safety, health, and efficient performance at work.

Union Relevance

The RS provides trade unions with a clear guide to the standards that companies must follow regarding risk prevention, worker safety, and occupational health, including when digital technologies are involved.

Law on Protection against Employment Discrimination (LPED)

The LPED, in force since 1995, applies to all workers in the country, including those in both the public and private sectors. The law covers every stage of the employment relationship, from recruitment and hiring to promotion, job tenure, and possible dismissal.

The LPED establishes a key principle: no one can be discriminated against in the workplace. This means that no decision regarding hiring, task assignments, salary, promotion, or dismissal can be based on personal characteristics such as sex, age, race, sexual orientation, health status, disability, or any other factor that affects equality and human dignity.

The law is also relevant in a context where an increasing number of hiring, management, and evaluation processes are carried out through digital technologies, offering protection against digital discrimination.

Companies must ensure that the technological tools they use to select or evaluate workers do not reproduce biases or exclude any person or group, whether directly or indirectly.

Workers should know that:

→ **Protection Against Discrimination (Art. 1)**. No person can be rejected, displaced, or treated unequally when seeking or keeping a job for personal, family, or social reasons, even when these actions are carried out through digital means.

→ **Prohibition of Discriminatory Medical Requirements (Art. 2).** It is illegal for a company to require medical exams or certificates related to pregnancy, sterilization, fertility, or any other personal condition unrelated to the job duties, even if this is done through digital tools.

→ **Remedies for Discriminatory Dismissal (Art. 4)**. If a worker is dismissed for discriminatory reasons, they have the right to choose between two options: getting their job back, with full payment of the wages they lost, or receiving double the salary corresponding to the period they were out of work, plus compensation for moral damages.

→ **Reversal of the burden of proof (Art. 818 of the CLL).** If the employee cannot directly prove that discrimination occurred because they lack the objective means to do so, the employee may ask the judge to reverse the burden of proof. In that case, the employer must provide evidence showing that no discriminatory act took place.

→ **Art. 1 of the LPED**
It defines the grounds for discriminatory practices and prohibits them throughout the entire employment relationship.

→ **Art. 2 of the LPED**
It defines discriminatory practices related to medical aspects and establishes penalties.

→ **Art. 4 of the LPED**
It sets out employees' rights in cases where the employment relationship is terminated for discriminatory reasons.

→ **Art. 818 of the CLL**
It regulates matters related to the burden of proof. It stipulates that in certain cases the burden may be reversed.

Union Relevance

The provisions of this law may be invoked by trade unions in response to any company decision that presents a discriminatory bias, including when such actions are carried out through digital means. Article 1 is very clear in defining when such bias may be established. In addition, Article 4 provides trade unions with tools to act in cases of discriminatory dismissals.

General Law on the Protection of Personal Data (LPPD)

The LPPD, in force since 2018, protects individuals' rights against the misuse of their personal information, including cases in which such misuse occurs through digital means.

Although it is not exclusively or explicitly focused on labour relations, the law fully applies to them because companies handle employee data through digital technologies at every stage of the employment relationship: during recruitment and hiring, throughout employment, and at termination.

Its provisions cover both private- and public-sector workers.

The LPPD establishes a key principle: A worker's personal data belongs to that worker, and no one may use it without a legitimate basis. In the workplace, this requires employers to treat workers' information with transparency, respect, and adequate security measures.

A company may not collect, share, or analyse workers' data beyond what is necessary for legitimate work-related purposes.

Workers should know that:

→ **Lawful Use of Personal Data (Art. 7)**. Their personal data can only be used when there is a legitimate reason. This may include, for example, the worker's explicit consent, compliance with a legal obligation, fulfilment of a contract, or protection of their health. If none of these reasons exist, your employer cannot request or process your personal information.

→ **Right to Information About Worker's Data (Arts. 9 and 18).** Workers have the right to know what data their employer is collecting, for what purpose it is used, who has access to it, and how long it is kept. This information must be provided clearly and transparently, even when the data are processed through digital or automated systems.

→ **Duty to Protect Personal Data (Art. 46).** The company must protect workers' personal information and keep it secure. It is required to adopt technical and administrative measures to prevent leaks, losses, or unauthorized access.

→ **Right to Human Review of Automated Decisions (Art. 20)**. If a decision affecting a worker, such as a performance evaluation or a work profile assessment, was made by an automated system, the worker has the right to request a human review and to receive an explanation of the criteria used.

→ **Obligation to Prepare a Data Protection Impact Report (Art. 38)**. The national authority (National Data Protection Authority) may require the company

to prepare a data protection impact report (DPIR), including for sensitive data, regarding its processing operations. The report must be prepared in accordance with applicable regulations and must respect commercial and industrial confidentiality. The report must contain, at a minimum, a description of the types of data collected, the methodology used for collection and for ensuring the security of the information, and the controller's analysis of the measures, safeguards, and risk-mitigation mechanisms adopted.

→ **Special Protection for Sensitive Data (Arts. 5 and 11)**. Sensitive data receives stronger protection. They can only be used in justified cases and under strict conditions of confidentiality. Under the law, sensitive data include personal information on racial or ethnic origin, religious beliefs, political opinions, trade union membership or membership in religious, philosophical, or political organizations, as well as data related to sexual life or health, and genetic or biometric data.

→ **Art. 1**
It expresses the commitment to protect the processing of personal data, including when carried out through digital means, to safeguard the fundamental rights to freedom, privacy, and personal development.

→ **Art. 2**
It sets out the foundations of data protection. These include privacy, self-determination, freedom of expression, and respect for human rights.

→ **Art. 5**
It sets out a series of definitions, including that of sensitive personal data. Under the law, sensitive personal data include, for example, trade union membership.

→ **Art. 7**
It specifies the circumstances under which personal data may be processed.

→ **Art. 9**
It grants the data subject the right to access information concerning the processing of their personal data.

→ **Art. 11**
It sets out the circumstances under which the data defined as sensitive in Article 5 may be processed.

→ **Art. 18**
It grants the data subject the right to know what is done with their personal data and how it is used.

→ **Art. 20**
It establishes the right to a careful human review of decisions made by automated systems that use personal data as input.

→ **Art. 38**
It states that the national authority may require data controllers to prepare a data protection impact report.

→ **Art. 46**
It requires data controllers to adopt appropriate security measures.

Union Relevance

Today, workplaces are increasingly incorporating a wide range of digital technologies that collect workers' personal data. This occurs both in private companies and in governmental agencies. The technologies described in Section 2) of this report are examples of this trend. The LPPD provides protection in this regard. Under Articles 2, 5, and 7, trade unions may request that the company explain the reasons for processing employees' personal data. However, Article 20 offers what is perhaps the most significant protection: it allows workers' representatives to demand rational and well-founded explanations for decisions made by automated systems that use workers' personal data as input.

Law on the Use of the Internet (LUI)

The LUI, in force since 2014, applies to all individuals and institutions in the country, including both public and private entities. Although it is not exclusively or explicitly focused on labour relations, its principles also protect workers, since much of today's work activity depends on the use of networks, digital platforms, and online communication systems.

The main goal of the LUI is to ensure that the use of the internet preserves freedom, privacy, and, more broadly, the human rights of users. In the workplace, this means that companies and employers must handle workers' digital information transparently and with respect for their fundamental rights.

Workers should know that:

→ **Right to Privacy and Confidentiality (Arts. 7 item I–II).** They have the right to privacy, intimacy, and the confidentiality of their communications. No employer can access, disclose, or use their private information without justification or their consent.

→ **Protection of Workers' Personal Data (Arts. 7 item VII).** The processing of workers' personal data, including its collection, storage, or transmission, can only be done with the worker's free, explicit, and informed consent. They have the right to know what data are collected and for what purposes they are used.

→ **Limits on Digital Monitoring (Arts. 7 and 10).** Digital monitoring or control of work activities performed online must have limits. The company cannot monitor workers' communications or filter or analyse the content of workers' messages or browsing history, except in cases strictly necessary for technical or security reasons.

→ **Art. 2**
It states that the use of the internet in Brazil is primarily based on respect for freedom of expression.

→ **Art. 3**
It establishes, among the principles governing the use of the internet, the protection of privacy and the protection of personal data.

→ **Art. 7**
It sets out the rights that protect citizens when they navigate the internet. These include respect for their personal data and the inviolability of their privacy and communications.

→ **Art. 10**
It sets out the responsibilities of those in charge of storing internet browsing records and data.

Union Relevance

At present, various cybersecurity tools, such as the one mentioned in Section 2) of this report, may compromise the privacy of workers' internet browsing and electronic communications. The LUI provides trade unions with grounds to respond to the growing implementation of such cybersecurity technologies. For instance, if the company has access to workers' private communications, trade unions may invoke item III of Article 7 of the law to restrict such access.

Bill on the Use of Artificial Intelligence (BUAI)

The BUAI, currently under discussion in the Federal Congress, aims to regulate the development, implementation, and responsible use of artificial intelligence (AI) systems. The bill seeks to balance the protection of human rights, fundamental freedoms, dignity, and the value of human labour with the innovation introduced by AI technologies.

Workers should know that the BUAI:

- **Principles for the Development of AI (Art. 2)**. Seeks to ensure that the development of AI is based on principles such as equality, non-discrimination, and respect for workers' rights.
- **High-Risk AI Systems in Employment (Art. 17)**. Classifies certain AI systems as "high-risk" (subject to government oversight and regulation) particularly those used for recruitment, selection, screening, evaluation of candidates, promotion decisions, contract termination, task distribution, and performance or behaviour monitoring in employment, worker management, or self-employment contexts.
- **Right to Human Oversight and Explanation (Art. 8).** Guarantees direct human participation and oversight in AI implementation processes, as well as the right to clear information about how these systems operate. This means that anyone affected by an AI system may request an explanation of a decision, prediction, or recommendation, including information about the criteria, procedures, and main factors that influenced that specific outcome.

- **Arts. 1–3**
  These three articles outline the law's purpose and set out its underlying foundations and guiding principles. The law aims to strike a balance between safeguarding human rights, fundamental freedoms, dignity, and the value of human labour, and fostering the innovation brought about by AI technologies.
- **Art. 8**
  It states that any person affected by an AI system has the right to receive a clear, rational, and well-founded explanation regarding that impact.
- **Art. 17**
  It specifies which AI systems are considered high-risk. These include those used for recruitment, screening, filtering, and evaluating candidates; making decisions about promotions or the termination of employment relationships; assigning tasks; and monitoring and assessing the performance and behaviour of individuals affected by such AI applications in the areas of employment, worker management, and access to self-employment.

Union Relevance

The approval of this law would represent a major step forward in the discussion on the digitalization of workplaces. It could provide workers and their representatives with valuable arguments regarding the introduction of AI tools into work processes, particularly with respect to the protection of workers' fundamental rights. Trade unions should remain attentive to its progress through the legislative process.

Collective Bargaining Agreements Related to Digitalization

Based on the constitutional principle established in the CFRB, which protects workers against automation, numerous collective bargaining agreements have been signed.

In the absence of a specific law regulating this principle, collective negotiation plays a crucial role in addressing the introduction of digital technologies in the workplace.

Workers should know that the provisions negotiated and agreed upon in these agreements cover the topics detailed below. (Under each bargaining topic, an example of an agreed clause is included. Section 7, which contains the annex, includes all collective agreement clauses that refer to the digitalization of workplaces).

→ **Training and job retraining**. When new technologies are introduced that involve automation of production processes, companies must provide training opportunities, either internal or external, so that workers can gain the necessary skills for new work methods. The employer must cover all related costs.

For example, the Construction and Furniture Industry Union of São Paulo agreed that: "In the face of new technologies that involve the automation of production methods, companies commit to providing training so that their employees may acquire better qualifications in the new work methods."

→ **Monitoring of technological impacts**. The Internal Commission for the Prevention of Accidents and Harassment (CPAH) expands its role to include identifying and monitoring the effects of technological innovations, as well as making recommendations to improve outcomes and reduce associated risks.

For example, the Chemical Industry Union of Rio de Janeiro agreed that: "The CPAH shall have the authority to identify and monitor the impacts arising from the organization of production and work, as well as those resulting from technological and organizational innovations. It shall also present feasible proposals and measures to improve the work environment and continuously monitor their implementation, while being guaranteed access to all information necessary for the performance of its functions."

→ **Job reassignment in automation processes**. When companies adopt modernization processes or new production techniques, they cannot use these innovations as justification for dismissals. Workers whose positions are affected by modernization must be reassigned to other compatible roles.

For example, the Food Industry Union of Bahia agreed that: "The company shall not dismiss its employees covered by this agreement as a result of the introduction of new technologies or automation processes. It shall guarantee those affected by these changes the right to new training and functional redeployment, and it shall follow the same procedure in cases of rationalization, except in situations of force majeure."

→ **Communication and dialogue with unions.** Employers who plan to introduce new technologies must notify the unions in advance. Once notified, dialogue spaces should be established to discuss the nature and scope of the innovations, training needs, health and safety risks, and alternatives for reassigning workers who may be displaced by automation.

For example, the Rural Workers' Union of Pernambuco agreed that: "When employers decide to introduce new technologies, they shall notify the unions representing the professional category within the company's territorial base. The parties commit to creating a dedicated space for the specific discussion of new technologies, as well as for the training and retraining of workers who may be dismissed as a result of mechanization."

→ **Wage protection during technological innovation.** It is prohibited to reduce wages due to the introduction of new technologies or automation processes.

For example, the Food Industry Union of Santa Catarina agreed that: "Employees are guaranteed that, as a result of the introduction of new technologies, office automation, changes in work routines, or modifications to the production process that eliminate or alter their duties, they will receive company-funded training for other activities, and wage reductions are prohibited."

→ **Prohibition of dismissals due to automation**. The dismissal or replacement of workers as a direct result of implementing automated systems is explicitly prohibited.

For example, the Tourism and Hospitality Union of São Paulo agreed that: "In order to preserve jobs (...) the parties agree to prohibit the implementation and/or the dismissal or replacement of doormen by outsourced access-monitoring centers or 'virtual door keeping' systems."

Union Relevance

The negotiation topics described, inspired by the constitutional principle that protects workers against automation, serve as a reference for collective bargaining processes. Collective bargaining emerges as a key tool for safeguarding workers' dignity and ensuring the security and stability of their jobs.

Summary of laws currently in force

Table 1

Law	Coverage	In force since	Main Goals	Union Relevance	Key Articles
CFRB	All workers in the country	1988	Ensure decent, safe, and stable work	It enshrines the principle of protecting workers from automation	7, item 27
CLL	Private-sector workers and public-sector workers without a special statute	1943	Ensure decent, safe, and stable work	It regulates digital monitoring tools, telework, and matters related to health and safety at work, including in the context of the introduction of digital technologies	6, 75-A to 75-F, 157, 168, 166, 818
RS	Private-sector workers and public-sector workers without a special statute	1978	Establish the minimum conditions to prevent accidents, occupational illnesses, and harm to the physical or mental integrity of workers	The occupational risks they aim to prevent also include those arising from digitalization	RSs 1, 5, 7, 12, 17
LPED	All workers in the country	1995	It establishes that no one may be discriminated against in their workplace	The law is relevant in a context where an increasing number of hiring, management, and evaluation processes are carried out through digital technologies	1, 2, 4
LPPD	All Brazilian citizens (all workers in the country)	2018	Protects the rights of all individuals against the misuse of their personal information, including when such misuse occurs through digital means	Today, workplaces are increasingly incorporating a wide range of digital technologies that collect workers' personal data	1, 2, 5, 7, 9, 11, 18, 20, 38, 46
LUI	All Brazilian citizens (all workers in the country)	2014	Ensure that the use of the internet preserves freedom, privacy, and, more broadly, the human rights of users	Various cybersecurity tools may compromise the privacy of workers' internet browsing and electronic communications. The LUI provides trade unions with grounds to respond to the growing implementation of such cybersecurity technologies	2, 3, 7, 10

4.
Checklists of Questions You Have a Right to Ask!

You are not expected to be a technology expert in order to protect your rights at work. What matters is knowing which questions you are entitled to ask **before** a digital system is introduced and **while** it is in use. The following checklists translate existing legal rights into practical questions that workers and union representatives can use in discussions with management. Print these questions and keep them with you when preparing for, and meeting with, management about digital technologies. Their purpose is to help ensure that existing laws and rights are properly respected in the introduction and use of digital systems at work.

Checklist 1

Questions workers should ask before new technologies are introduced...

About safety, health, and dignity in the introduction of digital technologies

→ **Does the automated system the company plans to introduce respect workers' dignity, stability, and safety?**	→ Art. 7, item 27 of CFRB
→ **Is the technology the company will implement free from biases that could result in discrimination against workers, whether during hiring, throughout employment, or at termination?**	→ Art. 1 of LPED
→ **Do the digital technologies the company plans to use comply with workplace health and safety standards?**	→ Art. 157 item I of CLL
→ **Has the company conducted a comprehensive risk assessment related to the technologies it plans to introduce?**	→ RS 1
→ **Will employees receive training to prevent accidents and occupational illnesses related to the new digital technologies?**	→ Art. 157 item II of CLL
→ **Will the Internal Commission for the Prevention of Accidents and Harassment (CPAH) participate in identifying and evaluating the impacts of these technologies?**	→ Art. 163 of CLL and RS 5
→ **Will the company provide, free of charge, appropriate equipment and personal protective gear so employees can safely operate the new digital technologies?**	→ Art. 166 of CLL
→ **Will the company ensure that machines using digital technologies have physical protections, safety sensors, and emergency stop mechanisms?**	→ RS 12
→ **Will the company train employees who will operate the new digital machines and systems?**	→ RS 12
→ **Will the company conduct ergonomic assessments of workstations and adapt working conditions to workers' physical and psychological characteristics, considering the introduction of new technologies?**	→ RS 17

Regarding the implementation of telework or remote work supported by digital technologies

→ **Does the company recognize that employees working remotely through digital means have the same rights as those working in person at the workplace?**	→ Art. 6 of CLL
→ **Does the company acknowledge that digital tools used for supervision and monitoring have the same legal value as in-person supervision?**	→ Art. 6 of CLL
→ **If the company proposes switching an employee to a telework arrangement, will it provide or reimburse all necessary equipment and expenses required for remote work?**	→ Art. 75-D of CLL
→ **If the company proposes telework, will it respect the worker's right to disconnect outside regular working hours?**	→ Art. 75-B item 5 of CLL
→ **If the company proposes telework, will it ensure adequate health and safety conditions for remote work?**	→ Art. 75-B item 7 of CLL
→ **If the company proposes telework, will it offer training on how to prevent health issues or accidents related to remote work?**	→ Art. 75-E of CLL

Regarding digital technologies that collect and analyse employees' personal data

→ **What legal justification does the company invoke for introducing digital technology that collects and analyses employees' personal data?**	→ Art. 7 of LPPD and Art. 7 item 7 of LUI
→ **Does the company clearly and simply explain what personal data the new technology collects, for what purpose, who has access to it, and how long it is stored?**	→ Arts. 9 and 18 of LPPD
→ **Does the company guarantee effective security measures to protect workers' personal data from leaks, losses, or unauthorized access? Will the company reinforce those measures when handling sensitive data?**	→ Arts. 5, 11 and 46 of LPPD
→ **Will the company guarantee workers' right to request a human review and obtain explanations when a decision affecting them, such as a performance evaluation, is made based on digital analysis of their data?**	→ Art. 20 of LPPD
→ **Does the company request free, explicit, and informed consent before introducing any digital technology that collects, stores, or uses data from employees' internet browsing or electronic communications?**	→ Art. 7 item 7 of LUI
→ **Does the company set clear limits on digital monitoring and control over employees' internet use and electronic communications?**	→ Arts. 7 and 10 of LUI
→ **If the national authority (National Data Protection Authority) requested a data protection impact report (DPIR) from the company, did it comply with its obligation?**	→ Art. 38 of the LPPD
→ **Does the DPIR meet the minimum requirements of containing a description of the types of data collected, the methodology used for collection and for ensuring the security of the information, and the controller's analysis of the measures, safeguards, and risk-mitigation mechanisms adopted?**	→ Art. 38 of the LPPD

Questions that should be asked periodically after the implementation of new technologies

About safety, health, and dignity in the introduction of digital technologies

→ **Does the automated system introduced by the company continue to respect workers' dignity, stability, and safety? How has management assessed this?**	→ Art. 7, item 27 of CFRB
→ **Do the digital technologies used by the company in work processes show any biases that could lead to discriminatory practices against workers, whether during hiring, throughout employment, or at termination?**	→ Art. 1 of LPED
→ **Does the company fulfil its obligation to periodically review safety conditions and assess the risks arising from the use of digital technologies in work processes?**	→ RS 1
→ **Does the company regularly monitor the health risks that the use of digital technologies may pose to workers?**	→ RS 7
→ **Does the Internal Commission for the Prevention of Accidents and Harassment (CPAH) have access to the results of digital risk assessments?**	→ Art. 163 of CLL and RS 5
→ **Is the CPAH kept informed about changes in the nature and scope of the digital technologies used by the company?**	→ Art. 163 of CLL and RS 5

Regarding the implementation of telework or remote work supported by digital technologies

→ **If the worker needs new tools or equipment to perform telework or remote work using digital technologies, does the company provide them?**	→ Art. 75-D of CLL
→ **If the worker incurs additional expenses while performing telework or remote work using digital technologies, does the company reimburse those costs?**	→ Art. 75-D of CLL
→ **If the company intends for the worker to leave the telework arrangement and return to on-site work, does it negotiate this change with the worker and provide notification in accordance with legal requirements?**	→ Art. 75-C item I of CLL

Regarding the implementation of digital technologies that collect and analyse employees' personal data

→ **Does the company inform workers about any changes in the nature of the digital technologies used to collect and analyse personal data, or in the methods these technologies use for such collection and analysis?**	→ Arts. 9 and 18 of LPPD
→ **If the company makes decisions about workers based on the automated analysis of their personal data, does it provide clear explanations of the reasoning and criteria used to reach those decisions?**	→ Art. 20 of LPPD
→ **Can it be verified that the cybersecurity system used by the company does not infringe on employees' privacy, such as their internet browsing activity or electronic communications?**	→ Arts. 7 and 10 of LUI

5.
Filling the Gaps – Bargaining Topic Suggestions

Existing law does not fully address many of the practical problems created by AI, monitoring technologies, and data-driven management at work. Collective bargaining is therefore an important way for unions to address these gaps. This section provides examples of negotiating themes that unions may draw on when developing their own demands to regulate how digital systems affect working conditions.

The collective bargaining agreements mentioned in Section 3, page 17, provide examples of negotiation topics inspired by Article 7, item 27, of the CFRB. In the below additional potential negotiation topics are suggested aimed at expanding worker protection in the face of challenges brought by digitalised work environments.

Workers' Right to Non-Discrimination in the Workplace

Workers have the right not to be discriminated against at any stage of their employment relationship. In this regard, some relevant negotiation topics could include:

- **Transparency in the criteria used by digital technologies that make decisions affecting workers**. For example, if a company introduces a system that automatically assigns shifts or tasks, it must disclose what variables the system considers and how they are weighted to rule out possible discriminatory biases.

- **Creation of a review procedure for decisions made by digital technologies that may involve discrimination.** For example, if a worker believes they were unfairly affected by a decision guided by a digital system, such as a dismissal, denial of promotion, or pay reduction, the worker and their representatives must have access to the data used to make that decision and participate in its review together with the company.

Workers' Right to Ergonomic Conditions Adapted to Their Needs

Workers have the right to ergonomic conditions suited to their personal characteristics. In this regard, a relevant negotiation topic could be:

- **Implementation of participatory and periodic ergonomic evaluations of digital workplaces, with worker and union participation**. For example, remote workers could review their home workspace conditions with the company every six months to negotiate improvements such as regular breaks, short stretching or movement pauses, and the provision or adjustment of ergonomic furniture to prevent visual or musculoskeletal problems.

Workers' Right to the Proper Use of Their Personal Data

Workers have the right to ensure their personal data are not misused. In this regard, relevant negotiation topics could include:

- **Secure and transparent mechanisms for handling employee data collected through digital technologies**. For example, if a company uses tracking or telemetry tools to monitor the location of drivers or delivery workers, it must inform each worker in writing about what data are processed, for what purposes, who has access to them, and how long they are stored. It must also explain the legal basis for collecting the data (such as employee consent, contractual obligation, or legal requirement) and guarantee technical safeguards against unauthorized access, loss, alteration, or disclosure.

- **Workers' free access to their own data stored in company digital systems**. For example, if the company uses a mobile app to track working hours and productivity, employees should be able to access their own data and understand how they are analysed or evaluated.

- **Limits on data access outside working hours**. For example, if tracking or telemetry technologies are used for drivers or couriers, their use must be restricted to working hours. Data collection outside that period would constitute an unlawful intrusion into the worker's private life.

- **Review of automated decisions based on worker data**. For example, if a company makes decisions affecting employment status, such as sanctions, task assignments, performance evaluations, or dismissals, based on automated data analysis, the worker has the right to request a human review, to know the criteria used, and to contest the decision if they believe it is unfair.

- → **Limits on cybersecurity systems and respect for worker privacy**. For example, if the company employs cybersecurity tools to prevent cyberattacks or data leaks, these tools must not intrude into workers' browsing histories or personal communications.

- → **Union audits on company data practices**. For example, companies should be required to report annually to unions on how they manage employee personal data, what data they collect, on what legal basis, where they store it, how they protect it, and for what purposes it is used. In addition, unions could also demand that workers be granted the right to prohibit the company from selling their personal data.

Company Obligations for Worker Health and Safety

Companies must not only ensure the health and safety of their workers but also facilitate regular inspections by the relevant authorities. In this regard, relevant negotiation topics could include:

- → **Expanding the scope of inspections to digital work environments**. For example, workplace health and safety inspections should include the review of digital technologies used at work, identifying risks associated with their intensive use, such as excessive surveillance or stress caused by constant performance monitoring systems.

- → **Worker and union participation in inspections**. For example, workers and their representatives should be able to actively participate in inspections of digital environments, review reports issued by oversight authorities, assess risks, and follow up on their proper mitigation.

6.
Summary Reflections

If you remember only one thing from this report, remember this: digital systems do not remove your rights – they give you new reasons to use them!

In Brazil, the legal and labour framework offers a relatively good level of protection for workers against the digitalization of workplaces. Even so, it is a framework that can be improved. Part of the existing regulation was designed before the widespread adoption of digital work environments and therefore lacks the specificity needed to address today's technological transformations. One example is the LPED, enacted in 1995, which does not include direct provisions on the discriminatory biases that automated systems may produce. Additionally, some legislation, although capable of being adapted to workers' needs, does not directly address employment relations. A clear example is the LPPD: its primary purpose is the protection of personal data, but it does not regulate employment relationships with precision, nor the specific issues that arise from the use of digital technologies in the workplace.

The current framework also fails to fully address, or does not address at all, certain issues that are particularly relevant in digital capitalism, such as the development of artificial intelligence (AI) systems, the specific situation of platform workers, or the sophisticated surveillance and control mechanisms that constantly monitor workers' activity.

Within this context, two possible paths emerge to overcome these limitations.

→ The first involves creating forward-looking legislation that responds to the needs and demands of workers in the face of ongoing transformations. One example of this path, at least potentially, is the bill aimed at regulating the development, use, and implementation of AI, seeking to reconcile the protection of rights, fundamental freedoms, human dignity, and the value of labour with the innovation introduced by these technologies. Another example lies in the legislative intent to regulate the constitutional article that protects workers from automation, an initiative based on the conviction that it is necessary to introduce checks and balances into digitalization processes to ensure that workers are not harmed and have better conditions to face the professional and personal transitions imposed upon them.

→ The second path is collective bargaining, which, under constitutional protection, has become a fundamental and effective tool for safeguarding workers in areas where the law does not yet provide direct solutions. As seen in section 3, page 16 f, in the absence of a specific law as required by the Constitution, collective bargaining serves as a mechanism for regulating the constitutional principle that protects workers from the impacts of automation. In this regard, several collective agreements have addressed key issues related to the introduction of new technologies in the workplace, such as the obligation of prior dialogue between companies and unions; the training, retraining, and reassignment of workers affected by technological changes; the monitoring of technological impacts; wage protection during innovation processes; and the prohibition of dismissals linked to automation. Likewise, the examples discussed in Section 5 illustrate a similar trend: they show how collective bargaining can adapt older legal clauses, written before the digitalization of work, to the current needs of workers. It is important to highlight that, for future collective bargaining to be truly effective and as successful as the examples discussed, both trade unions and employers must have an adequate level of knowledge about the potential benefits and risks that digital technologies introduce in the workplace.

Technological progress in the labour field must respect the principles of social justice. Innovations should contribute to improving working conditions and workers' quality of life, rather than deepening exploitation or precariousness. In discussions on the digitalization of work, workers and their organizations must be able to participate actively, supported by a legal and labour framework that guarantees such participation and protects their rights.

In Brazil's case, as noted, this legal structure, while adaptable to present needs, can still be improved. Legislative initiatives are under discussion, yet significant gaps persist that limit the protection of workers against the risks posed by digital technologies. In this scenario, collective bargaining emerges as the most immediate and effective tool for addressing these challenges. However, it is the combination of strong collective agreements and forward-looking legislation that would enable a digitalization process grounded in transparency, effective safeguards, and social justice.

7.
Annex – Links to the Laws and Agreements Covered

→ **Constitution of the Federative Republic of Brazil (CFRB)**
Link: https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm

→ **Bill no. 4035, of 2019**
Regulates item XXVII of Article 7 of the Federal Constitution, to provide for the protection of workers in the face of automation processes (BRPPA)
Link: https://www25.senado.leg.br/web/atividade/materias/-/materia/137793

→ **Case no. TST-RR-11307-80.2019.5.15.0053**
Link: https://www.conjur.com.br/wp-content/uploads/2024/05/tst-acordao-portaria-virtual.pdf

→ **Decree-Law no. 5.452, of May 1, 1943**
Consolidation Of Labour Laws (CLL)
Link: https://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm

Regulatory Standards of the Ministry of Labour and Employment (RS)

→ **RS 01**
General Provisions and Occupational Risk Management
Link: https://www.gov.br/trabalho-e-emprego/pt-br/acesso-a-informacao/participacao-social/conselhos-e-orgaos-colegiados/comissao-tripartite-partitaria-permanente/normas-regulamentadora/normas-regulamentadoras-vigentes/nr-01-atualizada-2024-i-1.pdf

→ **RS 05**
Internal Commission for the Prevention of Accidents and Harassment (CPAH)
Link: https://www.gov.br/trabalho-e-emprego/pt-br/acesso-a-informacao/participacao-social/conselhos-e-orgaos-colegiados/comissao-tripartite-partitaria-permanente/normas-regulamentadora/normas-regulamentadoras-vigentes/norma-regulamentadora-no-5-nr-5

→ **RS 07**
Occupational Health Medical Control Program (OHMCP)
Link: https://www.gov.br/trabalho-e-emprego/pt-br/acesso-a-informacao/participacao-social/conselhos-e-orgaos-colegiados/comissao-tripartite-partitaria-permanente/normas-regulamentadora/normas-regulamentadoras-vigentes/norma-regulamentadora-no-7-nr-7

→ **RS 12**
Safety at Work with Machinery and Equipment
Link: https://www.gov.br/trabalho-e-emprego/pt-br/acesso-a-informacao/participacao-social/conselhos-e-orgaos-colegiados/comissao-tripartite-partitaria-permanente/normas-regulamentadora/normas-regulamentadoras-vigentes/norma-regulamentadora-no-12-nr-12

→ **RS 17**
Ergonomics
Link: https://www.gov.br/trabalho-e-emprego/pt-br/acesso-a-informacao/participacao-social/conselhos-e-orgaos-colegiados/comissao-tripartite-partitaria-permanente/normas-regulamentadora/normas-regulamentadoras-vigentes/norma-regulamentadora-no-17-nr-17

→ **Law no. 9,029, of April 13, 1995.**
Prohibits the requirement of pregnancy and sterilization certificates, and other discriminatory practices, for the purposes of admission or continuation of the legal employment relationship, and provides other measures (LPED)
Link: https://www.planalto.gov.br/ccivil_03/LEIS/L9029.HTM

→ **Law no. 13.709, of August 14, 2018**
General Law on the Protection of Personal Data (LPPD)
Link: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

→ **Section 3) page 15. Law no. 12,965, of April 23, 2014.**
Establishes principles, guarantees, rights, and duties for the use of the Internet in Brazil (LUI)
Link: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

→ **Section 3) page 16. Bill No. 2338, of 2023**
Provides for the use of Artificial Intelligence (BUAI)
Link: https://legis.senado.leg.br/sdleg-getter/documento?dm=9347593&ts=1742240889254&disposition=inline

→ **Collective agreements with clauses relating to the digitalisation of work environments**
Source: DIEESE (Inter Union Department of Statistics and Socioeconomic Studies)
Link: https://www.gov.br/trabalho-e-emprego/pt-br/boletim-boas-praticas/pdf/boletim-boas-praticas-dieese_09-inovacoes-tecnologicas.pdf/

8.
Glossary List

This glossary explains recurring terms and concepts used throughout the country chapters. It is intended to support workers and union representatives in quickly understanding technical, legal, and managerial language commonly used in discussions about digitalised workplaces.

A

Algorithmic management The use of software systems and algorithms to allocate tasks, evaluate performance, determine pay, schedule work, or discipline workers, often with limited transparency or human oversight.

Artificial intelligence (AI) Computer-based systems designed to perform tasks that typically require human judgment, such as decision-making, pattern recognition, prediction, or classification. In workplaces, AI is increasingly used in recruitment, performance management, surveillance, and automation.

AI systems (Artificial Intelligence systems) An AI system is a type of digital system that uses computational methods such as machine learning, statistical models, or rule-based algorithms to generate outputs including predictions, classifications, recommendations, or decisions based on input data. AI systems are used in some workplaces for tasks such as recruitment screening, performance scoring, task allocation, or pattern recognition. AI systems are digital systems that use algorithmic models to generate outputs from data.

Automated decision-making (ADM) Decisions affecting workers that are made wholly or primarily by digital systems, with minimal or no human intervention, for example in hiring, scheduling, performance scoring, or dismissal.

B

Biometric data / biometric systems Personal data based on physical or behavioural characteristics, such as fingerprints, facial images, iris scans, or voice patterns, used to identify or authenticate workers, often for attendance, access control, or monitoring.

C

Collective bargaining Negotiations between workers' organisations and employers to determine working conditions, rights, and obligations. In the context of digitalisation, collective bargaining is used to regulate technology use where law is absent, weak, or insufficient.

Consultation and worker participation Legal or collectively agreed processes requiring employers to inform and involve workers or their representatives before introducing technological, organisational, or operational changes that affect working conditions.

D

Data Any representation of information, facts, or concepts in a form capable of being processed by a computer system.

Data Fiduciary / Controller The entity (usually the employer) that decides how and why personal data is processed and bears the legal responsibility for its protection.

Data Minimisation The principle that only the data strictly necessary for a specific, stated purpose should be collected and used.

Data protection Rules and principles governing how information relating to an identifiable person is collected, stored, used, shared, and retained. In workplaces, this includes amongst others attendance data, location data, performance metrics, and biometric information.

Data Protection Impact Assessment (DPIA) A structured assessment required in many jurisdictions before introducing high-risk data-processing systems. It evaluates risks to workers' rights and freedoms.

Digital labour platforms / platform work Work mediated through digital applications or online platforms that allocate tasks, manage performance, and process payment, often using algorithmic systems. Examples include ride-hailing, delivery, and online outsourcing.

Digital technologies Digital technologies are electronic tools, devices, software, and data-processing applications that create, collect, store, transmit, or analyse digital data. In workplaces, this includes items such as computers, mobile devices, biometric scanners, cameras, GPS devices, software applications, platforms, and databases. These technologies generate and process data that can be used in organising, monitoring, or managing work. Digital technologies are the individual electronic tools and applications.

Digital systems A digital system is an arrangement of multiple digital technologies that operate together to collect data, process it according to defined rules or instructions, and produce outputs. A digital system may include hardware, software, data storage, and interfaces used by managers or workers. The system refers to the combined operation of these components rather than any single device or application. Digital systems are combinations of digital technologies working together.

Digital surveillance / worker monitoring The use of digital tools to observe, record, or analyse workers' activities, movements, communications, or performance, including CCTV, GPS tracking, keystroke logging, and screen monitoring.

E

Enforcement gaps The disconnect between formal legal rights and their real-world application, often due to weak oversight, delayed remedies, limited access to regulators, or reliance on individual complaints.

F

Function creep The gradual expansion of a technology's use beyond its original stated purpose, for example when security or attendance systems are later used for performance evaluation or discipline.

H

Human oversight The requirement that automated or AI-driven systems remain subject to meaningful human review, judgment, and accountability, particularly when decisions affect workers' rights or livelihoods.

I

Informational asymmetry A power imbalance in which employers control access to information, data, and system logic, while workers lack insight into how technologies operate or how decisions are made.

O

Occupational safety and health (OSH) Legal and organisational obligations to protect workers' physical and mental well-being at work, including risks arising from stress, work intensification, constant monitoring, or technological change.

P

Platform worker classification The legal determination of whether platform workers are treated as employees, self-employed, or a separate category, which affects access to labour rights, social protection, and collective bargaining.

Power asymmetry An imbalance of authority and control between management and workers, intensified in digitalised workplaces through surveillance, data extraction, and algorithmic control.

Purpose limitation A core data-protection principle requiring that data collected for one specific purpose (e.g. security) not be reused for incompatible purposes (e.g. discipline or productivity scoring) without justification and consultation.

R

Right to explanation / transparency The principle that workers should receive clear, accessible information about what data are collected about them, how technologies function, and how decisions affecting them are made.

Right to disconnect The right of workers to be free from work-related digital communication and monitoring outside working hours, protecting rest time and work-life boundaries.

Risk assessment An evaluation of potential harms associated with introducing new technologies, including impacts on privacy, health, equality, workload, and job security.

S

Surveillance capitalism / data extraction A model in which value is generated by collecting and analysing large amounts of behavioural data, increasingly applied within workplaces through digital management systems.

W

Worker dignity and autonomy Foundational labour principles recognising workers as rights-bearing individuals, not merely data points or inputs, requiring limits on intrusive monitoring and automated control.

About the authors

Leonel Moya, Consultant, DataGénero, Argentina
Mailén García, Director, DataGénero, Argentina

Negotiating Digitalised Workplaces – Rights and Obligations

This series of country studies – encompassing to date Albania, Brasil, India, Ireland, Kenya, South Korea, and Uruguay – highlights the institutional power resources of workers to shape the digitalisation of workplaces. By knowing rights, laws and labour market agreements, workers and trade unions can henceforth better claim their rights and negotiate working conditions when digital technologies are introduced and used.

Further information on this topic can be found here:
↗ **fes.de/lnk/negodigirights**

Friedrich Ebert Stiftung