Scientific Research Publishing

Beijing Law Review, 2025, 16(4), 2442-2479
https://www.scirp.org/journal/blr
ISSN Online: 2159-4635
ISSN Print: 2159-4627

Data Protection and AI-Based Employee Monitoring: Legal Boundaries under Brazil's LGPD

Alexandre Pacheco da Silva, Carolina Britski Puga, Olívia de Quintana Figueiredo Pasqualeto

São Paulo School of Law, Getulio Vargas Foundation, São Paulo, Brazil
Email: alexandre.silva@fgv.br, carolpuga34@gmail.com, olivia.pasqualeto@fgv.br

How to cite this paper: da Silva, A. P., Puga, C. B., & Pasqualeto, O. de Q. F. (2025). Data Protection and AI-Based Employee Monitoring: Legal Boundaries under Brazil's LGPD. *Beijing Law Review, 16,* 2442-2479.
https://doi.org/10.4236/blr.2025.164125

Received: September 9, 2025
Accepted: December 6, 2025
Published: December 9, 2025

Abstract

This article provides an overview of how artificial intelligence (AI) is used to monitor employees in Brazilian companies, utilizing People Analytics tools. It analyzes HR Techs operating in Brazil to explore how the monitoring service is provided, the types of employee data collected, and the purposes of such collection. We aim to comprehend the potential hazards and boundaries of employee monitoring in Brazil under the General Personal Data Protection Act (LGPD). The incorporation of AI into monitoring tools has elevated the capability to evaluate employee conduct significantly due to the vast amount of data that is processed. Although employee monitoring is not new, the AI analysis component introduces new considerations for the preservation of individual data rights. In the age of big data, where personal information holds immense value for corporations, it is imperative to facilitate conversations around the boundaries of data processing in various sectors, taking into account the potential infringement of employees' privacy—particularly in remote work scenarios. The objective of this study is to evaluate how Brazilian legislation has reacted to this situation and to comprehend its limitations.

Keywords

Artificial Intelligence, People Analytics, Employee Monitoring, HR Techs, LGPD

1. Introduction

We are currently experiencing a period of significant technological advancement, during which technology is becoming increasingly prevalent in a variety of everyday activities. The global COVID-19 pandemic has accelerated the digital trans-

formation process that had already been underway for the previous decade, affecting working practices. Many companies have had to adapt to the remote work model and, consequently, to the digitization of work (Brito, 2024).

Companies now rely heavily on artificial intelligence (AI) to manage their workforce (Bar-Gil, Ron, & Czerniak, 2024). AI tools help screen job candidate selection, track performance and oversee daily tasks. Although employee monitoring itself is not new, AI-driven analytics have reshaped it by processing vast amounts of behavioral data in real time. Currently, the majority of this monitoring is conducted by HR Techs (Arbex, 2020), specialized companies that develop automated solutions for human resources processes to enhance the efficiency of the sector (Magalhães, 2025). By aggregating data from monitoring tools, these companies generate descriptive reports, predictive insights, and prescriptive recommendations in a practice known as People Analytics (Dias, 2019).

This issue has prompted numerous discussions, as evidenced by the recent media coverage. For instance, there are articles such as: "Companies use AI to monitor workers-45% of employees say it has a negative effect on their mental health," (Shrikant, 2023), "Amazon Watches Its Workers and Waits for Them to Fail," (Ashworth, 2023), and "How worker surveillance is backfiring on employers." (Morgan, 2023). These examples underscore an urgent question: where should the boundaries of employee surveillance lie in the age of algorithmic management?

The Brazilian General Data Protection Law (*Lei Geral de Proteção de Dados*—LGPD, in Portuguese) (Brazil, 2018), which took effect in 2020, has raised concerns regarding the handling of personal data, particularly within corporate settings. The extensive use of AI in the collection and analysis of large datasets is contributing to an increase in the complexity of compliance. Debates around data processing limits are well underway in Europe and the US, but are still in development in Brazil, reflecting the novelty of the issue and its likely expansion in the coming years.

In view of this panorama, this paper aims to: i) understand how People Analytics tools have been used to monitor employees by the main HR Techs operating in Brazil; ii) understand the risks and limits that arise from making decisions with the data collected; iii) analyse how Brazilian law has responded to this new approach; iv) explore which legal basis justify the processing of this personal data in the light of the LGPD; and v) understand the role of the National Data Protection Authority (ANPD), drawing a parallel with European decisions on the subject.

To achieve these goals, the methodology combined bibliographic research with document analysis of selected HR Techs (Privacy Policies and Terms of Use available on their websites). The work is divided into four sections. Part I presents a historical overview of employee monitoring, from the Industrial Revolution to the current use of AI in People Analytics, emphasizing real-time monitoring tools. Part II examines the risks and limitations of excessive data processing and decision-making by companies using HR Techs, in contrast with the right to privacy. Part III provides a systematic analysis of the leading HR Tech companies operating in Brazil, with a focus on their products and the types of employee data they

collect. Part IV delineates legal guidelines grounded in Brazilian legislation, addressing the pertinent legal basis under the LGPD, salient risks, and recommendations. It also examines the role of the ANPD in comparison to European data protection authorities under the GDPR.

2. People Analytics: Applying AI to Employee Monitoring

Employee monitoring is nothing new. It began during the Industrial Revolution when supervision was informal (Ajunwa, 2023: p. 337), and managers would oversee workers by walking the factory floor or positioning their desks to maintain direct visual control. Over time, the need for more systematic oversight gave rise to management theories. One notable theory was scientific management (Ribeiro, 2015), also known as Taylorism (Taylor, 1947). This approach aimed to improve productivity in rapidly growing capitalist enterprises by applying scientific methods (Braverman, 1987: p. 82), which required increased monitoring of individual workers (Ajunwa, 2023: p. 321).

Throughout the 20th century, technological advances—especially those following the digital revolution—transformed traditional monitoring practices into more precise, individualized ones. Taylorism's emphasis on measurement and control laid the foundation for today's data-driven management culture. Rather than supervising teams or departments, companies now focus on tracking individual performance (Ball, 2021: p. 89).

The shift was accelerated by the COVID-19 pandemic (Pan American Health Organization, 2023)[1]. Remote and hybrid work models became the norm (Zanatta & Mathias Brotero, 2023), raising new questions. How can employers ensure that remote workers are fulfilling their responsibilities? In response, companies have adopted digital monitoring tools, including software that tracks online activity and content accessed, time-tracking tools that measure task duration, attendance systems that log work hours, overtime, and absences, and platforms that manage workloads and set goals. These tools serve multiple purposes, including productivity analysis, performance evaluation, risk management, legal compliance, and protection against data leaks or sabotage[2] (Ekka, 2021).

In today's digital landscape, personal data is constantly generated through corporate systems, smartphones, and wearable technologies (Ajunwa, 2023), fueling the rapid growth of the employee monitoring industry (Privacy Affairs, 2023). The integration of AI has further expanded companies' ability to process and analyze behavioral data on a massive scale (Eurofound, 2020). This has led to more sophisticated—and often more invasive—forms of oversight, contributing to what some describe as a state of "permanent surveillance" (Aloisi & De Stefano, 2022:

[1]The World Health Organization (WHO) characterized the novel coronavirus (SARS-CoV-2) as a pandemic on March 11, 2020, and announced its end on May 5, 2023.

[2]Wearable technologies are electronic devices that collect user-specific data when worn as accessories, clothing, or implants on the body. In the context of employee monitoring, these technologies aim to quantify various worker attributes, including productivity, physical activity, health, emotions, and communication style.

p. 299).

This shift towards data-driven management is exemplified by the rise of people analytics, a data-driven approach to human resource management that uses large sets of quantitative data, rather than subjective judgments, to guide HR decisions and optimize business outcomes (Bodie, Cherry, McCormick, & Tang, 2017: p. 965). It is a continuous process that transforms workforce data into insights, enabling managers to make more objective decisions about productivity, performance, and talent (McCartney & Fu, 2022: p. 300).

It is also important to distinguish between "monitoring" and "surveillance". Monitoring typically refers to observing work-related activities, while surveillance implies the broader and often opaque tracking of personal behaviors, including those not directly tied to job performance. Consequently, surveillance carries a more negative connotation and raises serious concerns about employee privacy (Eurofound, 2020).

2.1. The Impact of Employee Monitoring and the Transformative Potential of People Analytics

Nearly 80% of U.S. companies use employee monitoring tools and productivity calculations for decision-making, performance analysis, workplace safety, legal liability protection, and defense against sabotage and intellectual property theft (Ribitzky, 2023). In Brazil, companies have also adopted monitoring systems, albeit more slowly. According to a Capterra survey (Capterra, 2022), 55% of Brazilian companies currently use these tools. The six main activities monitored by Brazilian companies today are: i) attendance control; ii) workload management; iii) time management; iv) computer activity; v) desktop analysis; and vi) digital communications analysis (Ziegler, 2023). A summary of these practices can be seen in **Table 1** below.

Table 1. Methods companies use to monitor employees.

Modality	Software Description
Attendance Control	Analysis of login/logout times, idle time versus active time, attendance at work, and days off
Workload Management	Definition of work schedules, task/action lists, goals, and KPIs
Time Management	Monitors time spent on individual tasks, projects, and work schedules
Browsing monitoring	Monitors internet access and calculates time spent on each webpage
Desktop analysis	Webcam surveillance, keystroke tracking (West, 2021), and screenshot capabilities show which websites or applications were accessed and for how long
Digital communications analysis	Monitoring of incoming and outgoing emails, instant messaging, and video conferences

Companies can use employee data collected by monitoring tools to perform analyses and evaluate teams. These analyses can be used to develop better solutions for recruitment, team well-being, talent retention, and performance man-

agement. The process of using software to automatically cross-reference collected data and perform diagnostics, predictions, descriptions, and prescriptions is called people analytics (Dias, 2019).

In recent years, this method of people management has become popular because it allows companies to optimize strategic decisions regarding their employees. AI has revolutionized people analytics by simplifying employee monitoring processes and enabling the collection, storage, and analysis of large amounts of employee data. Thus, AI-driven employee monitoring offers significant advantages in terms of performance tracking, risk management, and identifying opportunities for employee development.

One illustrative example of people analytics in action is the use of predictive attrition software powered by machine learning algorithms (Bar-Gil, Ron, & Czerniak, 2024). Such tools[3] integrate data from multiple sources, including employee demographics, tenure, performance evaluations, engagement surveys, and even patterns of absenteeism. By processing these datasets, the system can generate predictive models that flag[4] employees with a high likelihood of leaving the organization within a defined period. The analysis not only identifies risk factors—such as lack of career progression or declining engagement—but also provides actionable insights for managers, such as targeted training programs, tailored retention bonuses, or internal mobility opportunities. For employers, the gains are substantial: reducing turnover costs, preserving institutional knowledge, and strengthening workforce stability, all of which directly contribute to improved organizational performance and efficiency.

A 2020 LinkedIn report on key trends in people management (LinkedIn Talent Solutions, 2023) revealed that 48% of respondents plan to use machine learning to forecast human resources data in the coming years. Additionally, a 2018 Visier survey showed that organizations with advanced people analytics functions outperform emerging organizations, boasting 56% higher profit margins and a 22%

[3]In recent years, specialized companies have emerged that apply people analytics to predict potential employee exits, helping organizations anticipate and address retention risks. These solutions typically combine human resources data, performance indicators, and engagement metrics with machine learning models to identify employees most likely to leave and recommend targeted interventions. For instance, Infeedo's Amber platform focuses on predictive attrition by analyzing engagement and sentiment data, providing AI-driven recommendations to HR teams for proactive retention strategies. Worklytics, by contrast, integrates HRIS data with collaboration signals (such as email and meeting patterns) to detect early signs of disengagement and attrition risk, offering a broader organizational lens. Knime, while not a turnkey HR platform, delivers a customizable, low-code environment where HR departments can build predictive workflows using historical data, allowing greater flexibility but requiring more in-house expertise. Together, these tools illustrate the spectrum of people analytics solutions—from ready-made platforms with actionable insights (Infeedo), to integrated workplace analytics (Worklytics), to customizable machine learning workflows (Knime).

[4]For example, Infeedo's Amber platform operationalizes this process by combining periodic employee check-ins, sentiment analysis from open-text responses, and engagement pulse surveys. The system uses natural language processing and machine learning models to detect patterns of disengagement or dissatisfaction that correlate with higher attrition risk. Based on these signals, Amber generates predictive scores that flag employees most likely to resign within a given timeframe and provides HR teams with actionable recommendations—such as initiating personalized conversations, adjusting workloads, or offering development opportunities—to intervene proactively.

higher return on assets (Visier, 2018). Given the rise of this new sector, many companies now offer software solutions that use artificial intelligence to implement people analytics. Table 2 below summarizes the main products offered by these companies.

Table 2. Description of people analytics solutions.

Modality	Product Description
Recruitment and Selection	Use data analysis tools to identify the most suitable candidates for specific positions based on their skills, experience, and background
Talent Retention	Identifying factors that contribute to employee turnover and developing strategies to retain talent
Skill Development	Analysis of performance and training data to identify skill gaps and enable the creation of customized development programs
Performance Management	Identifying factors that influence employee performance and implementing measures to improve overall team performance
Organizational Climate	Identifying areas of employee dissatisfaction and diagnosing measures to improve the culture and work environment
Strategic decision making	Collecting data to guide strategic business decisions such as team expansion, organizational restructuring, and resource allocation
Diversity and Inclusion	Assess diversity and inclusion within the organization to identify areas for improvement and develop strategies to promote a more inclusive environment

As shown in Table 2 above, people analytics tools support decisions related to recruitment, development, performance, organizational climate, and employee turnover. To enable these insights, companies monitor employees' activities and behaviors during working hours. Many people analytics providers offer real-time monitoring services, generating analyses and visual dashboards to guide decision-making. The main tools used for this type of monitoring are listed below:

Table 3. Description of tools used for real-time employee monitoring.

Tool	Description
Keylogger software	It records keystrokes and issues reports to supervisors. However, if employees use company devices for personal activities, such as accessing their bank accounts, this could expose their private information to supervisors.
Webcam	Using biometric data such as eye movements, body movements, and facial expressions, webcam software can assess whether people are paying attention to workplace tasks and meetings.
Geolocation tracking	Many company-issued electronic devices have geolocation features that allow employers to track their employees' physical movements and location. This generates data showing the locations and time spent on a given activity.

Continued

Web Browsing and Application Usage	Software monitors employees' activities, speed, and productivity. It shows which websites employees have visited and which applications they have used. This allows companies to track browsing behavior and see if employees are wasting time or visiting inappropriate websites. Additionally, companies can monitor application usage to assess productivity and policy compliance.
Email and social media monitoring	Emails are legally subject to company oversight to ensure that employees comply with company policies, refrain from engaging in illegal activities or leaking information, and avoid using company equipment for abusive or harassing actions. Companies can use keyword searches to identify suspicious or unethical activities and monitor attachment downloads.

A deeper analysis of Table 2 and Table 3 highlights that the main advantage for employers lies in the ability to better understand their workforce and, from there, tailor management strategies to maximize productivity and reduce organizational risks. By linking the categories of people analytics in Table 2 with the monitoring tools in Table 3**,** it becomes clear that the value of these solutions is not merely in collecting large volumes of data, but in transforming these raw inputs into actionable insights. For instance, retention strategies benefit when attrition-prediction models combine turnover statistics with monitoring data about employee engagement, such as patterns of absenteeism or declines in digital communication frequency. In this way, the employer gains a more accurate diagnosis of which employees are most at risk of leaving and can act preventively, avoiding replacement costs and preserving institutional knowledge.

It is equally important to note that the choice of monitoring tool depends on the specific organizational objective. If the company is concerned with improving training programs and addressing skill gaps, as described in the "Skill Development" category, it may rely more heavily on performance management software and application usage monitoring, which track how employees interact with learning platforms and productivity tools. Conversely, if the focus is on organizational climate and inclusion, surveys and communication monitoring may provide richer insights, pointing to dissatisfaction or discriminatory practices within the workplace. As an example, while keyloggers may be effective in ensuring compliance with cybersecurity policies, they are not the appropriate tool for identifying training needs or promoting diversity, underscoring the necessity of aligning the technological instrument with the employer's strategic goal.

Finally, the integration of these systems raises concerns about opacity in their operation and the degree of transparency with which they are communicated to employees. Employers may deploy monitoring tools on company-issued devices or indirectly through applications embedded in productivity platforms, often without workers' full awareness (Bar-Gil, Ron, & Czerniak, 2024) of the scope of data collection. This dual characteristic—of being simultaneously a management tool and a surveillance mechanism—amplifies the ethical and legal debates around privacy, consent, and autonomy in the workplace. In practice, while people ana-

lytics offers organizations powerful opportunities to optimize decision-making, it also demands careful governance and clear accountability regarding how these systems function, what data they collect, and how the resulting insights are applied to shape employees' professional lives.

2.2. Risks Involved in People Analytics

Employers monitor their employees for three main reasons (Ball, 2021: p. 89). First, they want to maintain productivity and track resource usage. Second, employers want to protect their corporate interests and trade secrets to prevent risks of defamation, sabotage, data theft, and hacking. Third, monitoring protects the company from legal liability by providing evidence in legal proceedings. These objectives are all legitimate and demonstrate that monitoring employees is necessary. Employees themselves also expect monitoring as a form of risk management that limits costs, protects value, and maintains service quality (Ibidem: p. 93).

However, problems arise when employee monitoring exceeds what is reasonable or necessary. In other words, problems arise when monitoring becomes excessive and turns into unprecedented surveillance. This occurs in two situations: 1) when employers monitor data outside the workplace, invading a non-professional dimension of the worker's life and 2) when they collect accurate and precise information on how employees use their time, thereby undermining their autonomy in performing their assigned tasks.

The first scenario—monitoring that extends beyond the workplace—may occur due to an expansion of the workplace beyond a physical location[5]. This makes it difficult to define what should or should not be monitored, which threatens to blur the line between work and non-work (Ajunwa, 2023: p. 322). For instance, if an employee works from home and is monitored via webcam or facial recognition systems, information beyond their professional scope may be collected. This could include details such as who they live with, whether they have children, and if they have a medical condition. For instance, a book about cancer on a shelf behind the employee's webcam could reveal this information. The same problem can arise with geolocation data because it provides access to personal information beyond the employer's monitoring authority, such as the neighborhood where the worker lives and the places they frequent.

A practical example of this intrusion can be seen when home-office monitoring tools capture data unrelated to an employee's professional activities. For instance, keylogger software installed on a company laptop may inadvertently record personal banking credentials or private communications conducted during breaks, while application monitoring might reveal frequent use of health-related websites that disclose sensitive medical conditions. Similarly, geolocation tracking could expose visits to religious institutions, political meetings, or even family residences,

[5]Brazilian law recognizes this issue, establishing that the home office work regime does not require monitoring. However, companies must enter into an agreement with their employees (Art. 75-B, §9 of the CLT).

all of which fall far outside the legitimate scope of workplace oversight. These forms of data collection, though incidental, transform employer surveillance into a mechanism that risks undermining personal privacy and autonomy, highlighting the need for clear boundaries between professional and private life.

Furthermore, the monitoring of employees' emails, instant messages, file transfers, typing patterns, printed documents, online meetings, and even social media activity—often conducted without meaningful consent (if it is possible to have free consent in an employment relationship, on which the worker is economically dependent)—can expose large amounts of sensitive personal information that go far beyond what is necessary for the employment relationship. Even when employers outline general monitoring practices, workers rarely perceive the full scope or depth of the data being gathered: how many categories of information are collected, which specific details are extracted, and what these ultimately disclose about their private lives. When the criteria for behavioral data collection are opaque, monitoring systems effectively operate as a black box, heightening the risk of capturing intimate and irrelevant information and blurring the boundary between legitimate workplace oversight and intrusive surveillance.

Another problem arises when employers demand and collect precise information about how their employees use their time. This undermines the employees' autonomy in performing their assigned tasks and can stimulate negative feelings at work (such as fear of performing tasks or even exacerbated competition in relation to colleagues) and illnesses (such as stress, or "technostress", and anxiety). Supervising work is part of an employer's managerial authority. This authority includes the power to direct employees' work (Maria, 2017), and it is guaranteed by Brazilian law[6]. This topic will be discussed in more detail in Part IV. The employment contract supports this managerial power by establishing the employee's subordination to the employer (Maria, 2017), which is also legally backed[7]. Given the requirement of subordination, it is reasonable to expect that an employee's autonomy to be reduced, as it is the duty of the contracting company to monitor the performance of assigned tasks.

However, excessive monitoring can infringe upon an employee's autonomy to perform their duties. This has negative implications for their ability to perform their tasks creatively. Employees tend to be less creative when they feel that their actions and communications are being monitored because they are concerned about how their actions will be judged (Brewer, 1995: p. 760; Larson & Callahan, 1990: p. 530). This can occur, for example, when employees know that the content of their emails, instant messages, file transfers, typing, printed documents, and online meetings are being monitored.

When employees are acutely aware that every action is being tracked, they may begin to self-censor, avoiding experimentation, risk-taking, or even minor mis-

[6]According to Article 2 of the Consolidated Labor Laws (CLT), the employer is responsible for "personally directing the provision of services by its employees."

[7]According to Article 482, Section h of the CLT, an employee may be dismissed for just cause if they fail to comply with their employer's orders.

takes that are part of the natural learning process. For instance, a software developer who knows their keystrokes and screen activity are being logged might hesitate to test unconventional coding solutions, fearing that failed attempts could be misinterpreted as incompetence rather than innovation. Instead of exploring new approaches or expressing candid opinions, workers may choose the safest course of action, limiting their willingness to innovate or engage openly.

Excessive monitoring can negatively impact employees for two primary reasons. First, it has the potential to compromise employee privacy, especially if employees do not authorize the disclosure of their information, which is then transmitted to unknown third parties (Lloyd, 2006). Second, the use of surveillance technologies can lead to "function creep" (Ball, 2021: p. 92), which occurs when people analytics tools produce more information than intended that can be used for purposes other than the intended monitoring.

This illustrates that the information gathered through employee monitoring can offer insights into not only their professional conduct to their personal lives. This issue is further exacerbated when this information is used to make decisions about compensation or advancement. These developments raise intricate concerns about privacy, personal space, the private sphere, reputation, and employees' image. Without a clear framework in place, employee monitoring can have serious repercussions, disrupting established work practices and adversely impacting existing levels of control, autonomy, and trust between workers and the company.

Furthermore, employee monitoring software can operate visibly, with employees aware their activities are being tracked, or invisibly, without their knowledge. A report by the Electronic Frontier Foundation (Fabro, 2022) revealed that many such tools are designed to avoid detection, raising serious concerns about the security and privacy of collected data. However, the use of such software gives rise to concerns regarding the security and privacy of the information companies collect. These risks are heightened when information is gathered without consent, particularly in remote work settings. As corporate surveillance technologies advance, they increasingly challenge the legal boundaries of acceptable monitoring practices.

3. A Study on People Analytics and HR Techs Operating in Brazil

Before you begin to format your paper, first write and save the content as a separate text file. Keep your text and graphic files separate until after the text has been formatted and styled. Do not use hard tabs, and limit use of hard returns to only one return at the end of a paragraph. Do not add any kind of pagination anywhere in the paper. Do not number text heads—the template will do that for you.

Finally, complete content and organizational editing before formatting. Please take note of the following items when proofreading spelling and grammar:

In Brazil, people analytics tools are generally used by hiring third-party companies, known as HR Techs. While many of these companies are American, there are already some Brazilian companies that provide monitoring tools for businesses. In

order to gain a more in-depth understanding of the methods of employee monitoring employed in Brazil, we have analysed sixteen HR Tech companies operating in the country. Our analysis has explored the products offered by these companies and the personal data collected for the purpose of providing services.

The companies were chosen based on research on websites about people analytics and monitoring[8]. To be included, they had to meet both of the following criteria: companies that offer i) employee monitoring services and ii) people analytics solutions. The following companies were analysed: Sólides (Sólides, 2023), Factorial (Factorial, 2024), Mywork (Mywork, 2023), Teramind (Teramind, 2023), Kickidler (Kickidler, 2023), ActivTrak (ActivTrak, 2024), FocusRO (FocusRO, 2023), Hubstaff (Hubstaff, 2023), Time Doctor (Time Doctor, 2023), Monitoo (Monitoo, 2023), Monitask (Monitask, 2023), Ekran System (Ekran System, 2023), fSense (fSense, 2023), WE Controlio (Controlio, 2023), Clever Control (Clever Control, 2023) and Interguard (InterGuard, 2023).

It is important to emphasize that this study did not involve direct testing or technical evaluation of the tools themselves. Instead, our analysis focused on the examination of publicly available documentation released by the companies. To this end, we reviewed information disclosed on their official websites—such as Privacy Policies and Terms of Use—as well as materials published on their LinkedIn pages. This methodological choice allows us to identify recurring patterns and shared features across the products offered, without making claims about their internal functioning or practical performance.

To enhance the visualization of the selected HR technologies, the following summary table consolidates key information about the companies. It outlines the types of data they collect, the real-time employee monitoring tools they employ, and the specific people analytics solutions they make available. This synthesis provides a clearer comparison of their approaches and highlights the range of practices adopted across the sector.

A comparative analysis of the platforms listed in **Table 4** reveals significant differences in the scope and intensity of real-time monitoring. On one end of the spectrum, companies such as Sólides and Factorial emphasize employee management functions—recruitment profiling, climate surveys, and attendance tracking—using data collection primarily to guide strategic HR decisions. In contrast, platforms like Teramind, Kickidler, and ActivTrak adopt a far more intrusive approach, capturing extensive digital footprints that include emails, instant messages, keystrokes, and even screenshots. These systems blur the line between performance management and surveillance, presenting heightened risks of overreach into employees' personal spheres.

The analytical capabilities of the platforms also diverge in terms of objectives and granularity. For example, Mywork and Hubstaff focus on time and attendance monitoring, producing automated reports on overtime and productivity to support compliance and payroll efficiency. Meanwhile, Clever Control and WE Con-

[8]The research and analysis on the selected companies was conducted in September 2023.

trolio combine facial recognition, keystroke logging, and continuous screen recording to generate detailed behavioral maps of individual employees, producing highly granular analyses of workflow and performance. While these systems promise valuable managerial insights, they also introduce the possibility of disproportionate interference in workers' autonomy by documenting every action, often without the employee's explicit awareness.

Table 4. Summary table of RH Techs (Source: Elaborated by the authors).

Company	Data Collected	Real-time employee monitoring tools	People Analytics Solutions
Sólides	Name, e-mail address, telephone number, interests, company, position, location and social security number, behavioral data, provided directly by the data subject, by creating their account on the platform	Sólides creates a behavioural profile (Sólides Profiler) based on the data collected when recruiting employees. This identifies behavioural tendencies in each professional through four profiles: executor, communicator, analyst and planner.	Based on the collected data, the software creates a visual overview of employee perceptions of the company (climate survey), generates situational and demographic indices, and analyses employee performance.
Factorial	Full name, work email, ID number, social security number, date of birth, gender, nationality, telephone number, office to which you are assigned, time off policy, bank account number, working hours, salary, contract duration, full address, emergency contacts, time of entry and exit from work and duration. In addition, depending on the service contracted, it can collect geolocation data, biometric data and payment data.	Time and attendance control and absence management via webcam monitoring.	Performance evaluation and provision of data for business diagnostics.
Mywork	Full name, company name, personal documents (RG, CNH, CPF and/or CNPJ, PIS and Work Permit), date of birth, credit card and/or bank details, contact information (e.g. landline number, cell phone number, residence or domicile, e-mail address, among others), photos and social media profiles, information regarding the employee's entry and exit times, their photo and geolocation in the foreground and background, with their consent.	Time and attendance control, including holidays, absences and lateness, is managed through geolocation and the requirement to take a photo when marking time.	Preparing automated reports to help manage overtime and labour processes.

Continued

Teramind	First name, last name, billing and mailing address, e-mail address, telephone number(s), account name and password, and credit card information	Monitoring of user activity, including emails, instant messages, file transfers, typing, printed documents, and online meetings.	Behavioral analysis aims to protect confidential data and detect behavior indicative of data threats.
Kickidler	Does not provide this information	It records hours worked and monitors user activity, including emails, instant messages, file transfers, typing, printed documents, online meetings, and employee social media. It also records screen activity.	It automatically generates reports on employee productivity and reports incidents such as unauthorized data exchange with clients and misconduct with contractors.
ActivTrak	Contact information includes employee and company names, job titles, postal addresses, telephone numbers, fax numbers, email addresses, and information about the client company and services of interest to the user. User activity data includes the exact date and time the user first accessed a specific activity, a brief description of each activity, the amount of time the user spent on each activity, and the number of times the user performed an action. Screenshots, title bars, and window content of user activities, as well as the full URLs of the activities accessed in a browser.	The tool detects when employees are online, which applications are being used, and how much time employees spend on each application. It also detects USB device activity and unauthorized file sharing.	The tool creates analyses of trends and patterns in monitored users' behavior from the collected data, aiming to identify workflow bottlenecks and possible threats to company data security.
FocusRO	Name, email address, and phone number.	The program takes real-time screenshots (blurred, unblurred, and encrypted), tracks time spent on each task (idle time, meetings, and breaks), and reports on typing via email.	Based on the collected data, automated reports are produced that identify monthly work hours and productivity bottlenecks.
Hubstaff	Full name, email address, company, telephone number (optional), photo (optional), team size, and position.	The program accesses applications and URLs and takes periodic screenshots using a timer initiated by the user.	Automated reports are produced based on the data collected that diagnose employee productivity.
Time Doctor	Name, email address, photo, physical address, and payment information.	Time control on each task, including automatic screenshots, chat monitoring, and tracking of which applications and websites are being used, as well as the number of keystrokes and mouse movements (though it does not monitor content).	It creates reports that measure the time employees spend on each task and manage their performance.

Continued

Monitoo	It collects data on which programs and websites have been accessed, how much time has been spent on each task, and how much idle time there has been.	It secretly monitors detailed website and program usage histories by user, department, category, or computer. It controls working hours and idle time and blocks websites.	Customizable interactive reports and graphs are created from the collected data for productivity management and control.
Monitask	It tracks start and end times, screenshots, mouse and keyboard activity levels, active applications and URLs, and the selected project and task names and notes.	With user authorization, monitor the time spent on a particular task and take screenshots of the task's content.	Reports are created that analyze each employee's performance, allowing the company to make decisions regarding employee remuneration.
Ekran System	Contact data includes name, email address, company name, and telephone number. Monitoring data includes user and host names, keystrokes, clipboard text, application names, active window titles, uptime, visited URLs, clipboard contents, and connected USB devices.	Activity monitoring, access management, and identity management are performed with the employee's knowledge. The employee's screen is recorded, including data collection on application names, visited URLs, opened files, changed windows, keystrokes, and mouse use.	This data is sent to the Ekran System server for security analysis. Based on this analysis, alerts are created in real time for activities that are potentially malicious and/or suspicious. Additionally, Power BI reports are used for productivity analysis.
fSense	Data on user actions on the monitored computer includes the name of the application or website (including the server and URL), the date and time of use, the name of the user who performed the action, the type of device used, and the duration of the action. Data from recordings and screenshots is only collected with the user's consent.	Computer usage data is monitored through the collection of information such as the websites and applications visited and the time spent using each one. This is done through recordings and screenshots taken every thirty seconds.	Based on the collected data, fSense creates reports for productivity management and overtime control, automatically identifying existing bottlenecks.
WE Controlio	The program records the user name, email address, computer IP address, type of browser used, and the applications and websites accessed, as well as how long they are used.	The program works without the employee knowing he or she is being monitored. It records the screen uninterruptedly and takes screenshots. This allows the company to access which websites are used, the date and time of access, and what is typed. It can also access the content of emails and instant messages.	If an employee accesses prohibited sites, the company will be notified by email. Additionally, the collected data is used to automatically track productive and distracting activities and create reports that evaluate employee productivity.

Continued

Clever Control	Contact details: name, email address and telephone number. Data identifying the device used: IP address and browser information.	Facial recognition via webcam; logging of keystrokes; instant screenshots whenever the employee switches windows, visits a new website or copies something to the clipboard; tracking of internet usage and other installed programs; tracking of print jobs and external storage devices; and working time tracking, including idle time.	Based on the data collected, Clever Control automatically creates graphical representations and reports on the daily work routine of each member and team of the contracting company, enabling analysis of the workflow and detection of effective and/or ineffective patterns. Additionally, it generates reports on the most frequently used applications and website categories, the time spent on them, and how this figure changes over different periods.
InterGuard	Website usage data.	It tracks user login and logout times, as well as productive and unproductive time, and takes screenshots of the content accessed by the user.	InterGuard then uses this data to automatically generate productivity metrics, providing the contracting company with an overview of employee productivity.

Finally, the comparison shows that the choice of platform has direct implications for both organizational efficiency and employee privacy. Employers seeking to optimize performance management and identify bottlenecks may find solutions like fSense or Monitask sufficient, as they provide productivity dashboards and task-based reporting without extending into constant biometric or communication monitoring. However, when platforms such as InterGuard or Ekran System are deployed, the emphasis shifts toward security and risk management, with tools designed to detect suspicious behavior but at the cost of highly invasive data collection. This raises broader concerns not only about the proportionality of surveillance but also about the opacity of these systems, which are often embedded in company-issued devices without transparent disclosure, ultimately reinforcing the need for clear legal safeguards and governance structures.

Building on these findings, the next stage of the analysis turns to the broader risks highlighted in the previous chapter, with a focus on identifying where these technologies exceed their stated purposes. In particular, it is necessary to evaluate how likely they are to capture data unrelated to work activities and how such practices may erode worker autonomy. By assessing the balance between managerial benefits and the potential for intrusive oversight, we can highlight the specific risks that threaten employees' privacy.

Table 5 below presents a comparative overview of different HR Tech platforms, focusing on the risks they pose to employee privacy and autonomy. It highlights two main dimensions: the extent to which these technologies collect information beyond the workplace and the degree to which their monitoring practices may

undermine worker autonomy. By identifying invasive data collection techniques—such as geolocation, facial recognition, keystroke logging, and continuous screen recording—the table illustrates the varied levels of intrusiveness across platforms, providing a clearer picture of how each tool attempts to balance organizational efficiency with the protection of employee rights.

Table 5. Comparison between RH Techs in relation to the risks presented (Source: Elaborated by the authors).

Company	Collecting information outside the workplace	Risks	Harmful to worker autonomy	Risks
Sólides	Yes.	The collection of behavioral data	No.	N/A.
Factorial	Yes.	Facial recognition and geolocation	No.	N/A.
Mywork	Yes.	Facial recognition and geolocation	No.	N/A.
Teramind	Yes.	Employee activity is monitored in real time, including what is accessed and what is typed, and behavioral data is collected.	Yes.	Monitoring what is typed.
Kickidler	Yes.	Employee activity is monitored in real time, including what is accessed and typed, as well as screen recording.	Yes.	Monitoring of what is typed, and screen recording.
ActivTrak	No.	N/A.	No.	N/A.
FocusRO	Yes.	Screenshots and monitoring of what is typed.	Yes.	Screenshots and monitoring of what is typed.
Hubstaff	Yes.	Employee activity is monitored in real time, including what is accessed and screenshots. The timer is activated by the employee.	No.	N/A.
Time Doctor	Yes.	Employee activity is monitored in real time, including what is accessed and for how long, as well as screenshots and the number of keystrokes and mouse movements.	Yes.	Screenshots and the number of keystrokes and mouse movements

Continued

Monitoo	Yes.	Confidential monitoring of what is accessed and for how long by the employee.	Yes.	Confidential monitoring.
Monitask	Yes.	Employee activity is monitored in real time, including what is accessed and for how long, as well as screenshots.	Yes.	Screenshots.
Ekran System	Yes.	Employee activity is monitored in real time, including what is accessed and what is typed or handled. Screen recordings are made with the employee's knowledge.	Yes.	Monitoring of what is typed/handled, as well as screen recording.
fSense	Yes.	Employee activity is monitored in real time, including what is accessed and for how long, as well as recordings and screenshots.	Yes.	Recordings and screenshots.
WE Controlio	Yes.	Confidential monitoring of employee activity in real time, through uninterrupted recordings and screenshots. Notification to the company if the employee accesses prohibited websites without their knowledge.	Yes.	Confidential monitoring and making recordings and screenshots.
Clever Control	Yes.	Employee activity is monitored in real time, including what is accessed and for how long. Facial recognition, uninterrupted webcam recording, keystroke logging, and screenshots are also utilized.	Yes.	Uninterrupted webcam recording, keystroke logging and screenshots.
InterGuard	No.	N/A.	Yes.	Screenshots, which are anonymized and encrypted, accessed only by authorized persons.

The comparison shows a clear divide between companies whose tools are primarily limited to workplace-related data and those that extend far beyond this scope. For instance, Sólides, Factorial, and Mywork mainly rely on behavioral profiling, facial recognition, and geolocation, raising concerns about collecting information outside the professional context but without directly restricting worker autonomy. In contrast, platforms such as Teramind, Kickidler, and FocusRO not only monitor employee behavior in real time but also track keystrokes and screen activity, which directly impacts the ability of employees to work freely. These practices cross into highly invasive territory, as they create constant surveillance conditions where every typed word or opened file may be scrutinized, blurring the line between legitimate oversight and disproportionate control.

At the most intrusive end of the spectrum are platforms like WE Controlio, Clever Control, and Ekran System, which combine continuous webcam monitoring, keystroke logging, and detailed screen recording. These tools not only capture sensitive information unrelated to the job but also restrict employees' autonomy by creating an environment of total visibility. By contrast, companies such as ActivTrak and Hubstaff appear less invasive, as they do not engage in real-time collection of personal information outside the workplace and provide workers with greater awareness or control over when monitoring occurs. This variation underscores a critical tension: while some platforms can be framed as productivity management tools, others resemble surveillance systems that risk compromising trust, autonomy, and the balance of power in the employment relationship.

4. What Measures Does Brazilian Law Have in Place to Address These Risks?

4.1. Employee Monitoring: The Legal and Ethical Limits in the Age of Privacy

The use of artificial intelligence tools for employee monitoring is a relatively recent phenomenon, and in Brazil there is still no specific law regulating either AI in general or its application in the workplace. What does exist are broader provisions on the automated processing of personal data contained in the Brazilian General Data Protection Law (LGPD), as well as other data protection rules that may be applied by analogy. In this context, it becomes necessary to examine the current legal framework to determine which monitoring practices could be considered legitimate and which may exceed reasonable limits, particularly when evaluated against the principles and safeguards established by the LGPD.

The Brazilian Federal Constitution provides strong protections for individual rights in this area. Article 5, item X[9], establishes that intimacy, private life, honor, and image are inviolable, guaranteeing individuals the right to seek compensation for material or moral damages resulting from violations (Brazil, 1988). More recently, the right to the protection of personal data was expressly recognized as a

[9]Art. 5, X—Intimacy, private life, honor, and the image of individuals are inviolable, with the right to compensation for material or moral damages resulting from their violation being guaranteed.

fundamental right and incorporated into Article 5 under item LXXIX[10] (Constitutional Amendment No. 115, 2022). This constitutional framework reinforces the idea that the handling of personal information—whether by the State or private entities—must respect core principles of privacy and dignity, serving as a foundation for interpreting and applying data protection rules in Brazil.

Under Article 2 of the Brazilian Consolidation of Labor Laws (*Consolidação das Leis do Trabalho*—CLT, in Portuguese) (Brazil, 1943), employee monitoring is considered part of the employer's managerial and supervisory authority[11]. Paragraph 6 of Article 6 reinforces this by expressly allowing the use of technological tools to supervise work activities[12]. Moreover, Article 74, sections 1 and 2[13], requires companies with more than 20 employees to record and monitor attendance, specifically working hours. Together, these provisions establish a legal basis (or at least a presumption that it is legally possible) for employer oversight, while also setting boundaries on how monitoring should be conducted in practice.

In a 2020 decision, the Superior Labor Court (*Tribunal Superior do Trabalho*—TST, in Portuguese) held that employers may install surveillance cameras in shared workspaces, provided the equipment is placed in common areas and employees are duly informed in advance (Regional Labor Court of the 15th Region, 2023). The Court, however, imposed clear limits: cameras are strictly prohibited in locations intended for rest, as well as in spaces where privacy could be compromised, such as bathrooms and changing rooms. This ruling underscore the need to balance legitimate managerial interests in supervision with the fundamental right of workers to privacy and dignity in the workplace.

In contemporary office layouts, however, this separation between work and rest areas is not always clear-cut. Open-plan environments often include lounge spaces with sofas, beanbags, or other informal seating arrangements that serve simultaneously as areas for relaxation and as alternative workstations. In some cases, break areas are located within or adjacent to shared workspaces, making it difficult to distinguish where monitoring should legitimately occur. This architectural and functional overlap creates additional challenges for ensuring compliance with privacy protections, as surveillance devices placed in these settings may inadvertently capture moments intended for rest or personal interaction, thereby blurring the boundary between professional oversight and undue intrusion.

[10]The inclusion of item LXXIX was made through Constitutional Amendment No. 115 of 2022.

[11]Art. 2—An employer is defined as the company, whether individual or collective, which, assuming the risks of the economic activity, hires, pays, and directs the personal provision of services (emphasis added).

[12]Art. 6, Sole Paragraph—Telematic and computerized means of command, control, and supervision are equivalent, for the purposes of legal subordination, to personal and direct means of command, control, and supervision of another's work.

[13]Art. 74—Working hours shall be recorded in the employee register.

§ 2—In establishments with more than 20 (twenty) workers, recording the time of entry and exit is mandatory, whether through manual, mechanical, or electronic means, according to instructions issued by the Special Secretariat for Social Security and Labor of the Ministry of Economy, with prenotation of the rest period being permitted.

This illustrates that, under established legal and organizational traditions, the responsibility for monitoring lies primarily with the employer. Employers are granted the prerogative to adopt measures designed to safeguard company assets, ensure the physical safety of their workforce, and prevent misconduct such as sexual or moral harassment in the workplace. Yet, as noted in the challenges posed by modern office layouts—where rest areas and workstations often overlap—the exercise of this prerogative requires careful calibration. Without clear boundaries, surveillance intended to protect legitimate business and safety interests risks encroaching upon employees' spaces of rest and informal interaction, thereby intensifying tensions between managerial oversight and the preservation of individual privacy and dignity.

While labor courts and legislation recognize that employers can legitimately monitor their employees, they have also established clear limits on such monitoring. A regional labor court has ruled that companies must compensate employees and even reverse dismissals for cause when personal data is misused or employee privacy is violated (Pombo, 2023)[14]. These limits are based on the principles of proportionality and the safeguarding of employees' constitutional rights to privacy and intimacy.

However, as new technologies emerge, the boundaries of monitoring become increasingly blurred. There are cases in the Superior Labor Court that allow employers to monitor material provided to employees (e.g., company computers and corporate email accounts), but prohibit the monitoring of personal accounts and devices. However, employers must inform their staff that they are monitoring them and make them aware of the risks. On the other hand, there have been discussions about the feasibility of requests for disclosure of employee geolocation data to the contracting company for the purpose of proving compliance with working hours, without reaching a consensus on the matter. Many decisions emphasize the importance of informing employees and, when necessary, obtaining their consent for the processing of personal data. This ensures that such processing complies with established legal and procedural safeguards.

For employees, nevertheless, challenging monitoring practices that exceed what is reasonable under Brazilian law places them in a particularly difficult position. From one perspective, it is often nearly impossible for workers to fully grasp the extent of the monitoring to which they are subjected, especially given the complexity of the technologies involved and the frequent, opaque updates to the tools used by employers. From another perspective, even when employees recognize that surveillance may have crossed legal or judicially recognized boundaries, formally raising a complaint against the employer can be daunting, as it risks straining the employment relationship and exposing them to retaliation. This asymmetry of power underscores the vulnerability of workers in confronting excessive

[14]The Regional Labor Court of the 4th Region (TRT-4) overturned a dismissal for just cause and granted moral damages after an employer accessed private WhatsApp conversations among employees. This ruling reaffirmed the necessity of consent for processing personal data from private accounts.

monitoring and highlights the need for stronger institutional safeguards to ensure that employee rights are not undermined by the broad supervisory powers afforded to employers under Brazilian labor law.

In this context, Brazil enacted Law No. 13,709/2018, the General Data Protection Law (*Lei Geral de Proteção de Dados*—LGPD, in Portuguese), with the objective of establishing clear parameters for the processing of personal data and ensuring the protection of citizens' fundamental rights, particularly the rights to privacy and informational self-determination. Although approved in 2018, the LGPD only came into full effect in September 2020, marking a significant milestone in the Brazilian legal framework by aligning national data protection standards with global regulatory trends and providing a comprehensive basis for evaluating the legitimacy of data processing practices across both public and private sectors (Giuntini et al., 2021).

4.2. LGPD, Limits and Obligations to Ensure Privacy in the Workplace

The LGPD establishes principles and regulations for safeguarding personal data, including that of employees. The LGPD requires that data processing be based on a specific legal basis, carried out transparently and proportionately, and that data subjects be informed of the purposes of the processing and given reasons for it.
The LGPD's scope encompasses public and private companies that process personal data (Art. 1), with the stipulation that monitoring must be confined to work-related data (Segalla, 2021). Additionally, companies are prohibited from disclosing information obtained through monitoring (Segalla, 2021). When collecting personal data from its employees, the company generally acts as a controller, meaning it is responsible for making decisions regarding the processing of personal data (e.g., promotion, engagement, etc.). In contrast, HR Techs are responsible for collecting data and utilizing it to make predictions, acting as data processors. In essence, they handle the processing of employee data for the contracting company, while decisions about it are made elsewhere.

In order to process personal data, the controller must establish a corresponding legal basis, which will determine specific legal obligations that must be fulfilled by the controller. This obligation is based on the principle of necessity, according to which the processing of personal data must be restricted to the minimum necessary to achieve the intended purposes (Pestana, 2020). This means that data must be relevant, proportionate, and not excessive in relation to the purposes of the data processing.

Therefore, any data collected must be necessary to achieve a legitimate purpose, as outlined in Article 6, I of the LGPD. This means that data must be processed for "specific, explicit, and informed purposes, without the possibility of further processing in a manner incompatible with those purposes." Therefore, the most reasonable understanding is to justify the option for monitoring when the purpose of its processing cannot be fulfilled by other means that are less invasive to the

fundamental rights and freedoms of workers (intimacy and privacy).

As discussed in the previous chapter, implementing people analytics may lead to processing unnecessary personal data. For example, rather than monitoring all content accessed and/or typed by the employee to detect productivity bottlenecks and prevent distraction, as many HR tech companies do, information can be collected about which websites the employee accesses and for how long. For example, if an employee accesses their personal email account and receives a medical examination result, health data—which is considered sensitive—will be collected. However, this data is unnecessary to prevent distraction while performing professional tasks.

To avoid exceeding what is necessary, the LGPD requires the controller to identify and justify the applicable legal basis for processing personal data. As outlined in Article 7[15], processing personal data is permitted only when the following conditions are met: i) the data subject must give consent; ii) the controller must comply with a legal or regulatory obligation; iii) public administrations must process and share data to implement public policies outlined in laws and regulations or supported by contracts, agreements, or similar instruments; iv) research organizations must anonymize personal data wherever possible when conducting studies; v) processing is necessary for a contract or preliminary contract procedures in which the data subject is involved, at the data subject's request; vi) for regularly exercising rights in judicial, administrative, or arbitration proceedings; vii) for protecting the life or physical safety of the data subject or a third party; viii) for protecting health, exclusively in procedures performed by health professionals, health services, or health authorities; ix) when necessary for meeting the legitimate interests of the controller or a third party; and x) for credit protection.

The processing of sensitive data must be carried out with the explicit consent of the data subject, in a clearly defined and easily identifiable manner, for specific and explicit purposes (Art. 11, I). Alternatively, in the absence of consent from the data subject, processing may be conducted only in cases where it is absolutely necessary for the following items: i) the controller must comply with legal or regulatory obligations; ii) data must be shared for the public administration to implement public policies provided for in laws or regulations; iii) research bodies must conduct studies, ensuring the anonymization of data wherever possible; iv) rights must be exercised regularly, including in contracts and in judicial, administrative, and arbitration proceedings; v) protection of the life or physical safety of the data subject or a third party is paramount; vi) protection of health, exclusively in procedures performed by health professionals, health services, or health authorities, is a priority; vii) ensuring fraud prevention and the security of the data subject in the processes of identification and authentication of registration in electronic systems is essential.

A relevant distinction between the LGPD and the General Data Protection Reg-

[15]Article 7 (and Article 11 for sensitive data) of the LGPD establishes an exhaustive list that justifies the legitimate processing of personal data.

ulation (GDPR) of the European Union lies in the legal bases for processing that are unique to the Brazilian framework. Unlike the GDPR, the LGPD expressly includes credit protection as an autonomous legal basis (Art. 7, X), reflecting the strong role of consumer credit systems in Brazil and the need to regulate data flows connected to financial institutions and credit bureaus. Similarly, the LGPD establishes the implementation of public policies by public authorities (Art. 7, III) as a separate ground for processing, a basis not explicitly present in the GDPR, which addresses public interest in broader terms. Another point of divergence is the explicit mention of the protection of life or physical safety (Art. 7, VII), which, although indirectly encompassed under the GDPR's vital interests ground, is given independent and specific status in Brazilian law. Finally, in the context of sensitive personal data, the LGPD provides for fraud prevention and the security of the data subject in identification and authentication processes in electronic systems (Art. 11, II, g), which has no direct counterpart in the GDPR. These additional legal bases demonstrate how the Brazilian legislator tailored the LGPD to local economic and social realities, extending its scope beyond the more general grounds found in European regulation.

Therefore, when processing personal data—including sensitive data—companies must comply with the LGPD by grounding such activities in one of the legally recognized bases. As highlighted in the comparison with the General Data Protection Regulation (GDPR), the Brazilian framework offers a broader range of legal justifications, some of which are tailored to local realities, such as credit protection or the implementation of public policies. In the specific context of employee monitoring, however, the most relevant grounds tend to fall within four categories: i) the employee's consent; ii) the employer's legitimate interest in managing and supervising the workforce; iii) compliance with legal or regulatory obligations, such as labor law requirements; or iv) the execution of contractual duties arising from the employment relationship. These bases provide the legal foundation for processing data in pursuit of objectives like maintaining productivity, safeguarding corporate assets, and protecting the company against potential legal liability, while ensuring that such practices remain aligned with the principles of necessity, proportionality, and transparency established by the LGPD.

Consequently, legal bases other than consent do not require authorization from the data subject to process their personal data. However, according to the principles of transparency and accountability, individuals must be informed through a privacy notice that they are being monitored. The notice must clearly state what data is collected, the purpose of the processing, and the retention period. It must also be displayed in a prominent, easily visible location. This requirement clarifies that spyware, which monitors employees without their knowledge, violates the LGPD and is not advisable from a data protection perspective (Marques, 2022).

Furthermore, employers should not store data indefinitely, but rather for only as long as it serves the original intended purpose. The controller should establish

a retention period[16] for personal data collected for monitoring purposes and delete it once the processing purpose has been fulfilled.

Finally, data controllers and processors must maintain detailed records of their processing activities, with special attention to operations based on legitimate interest (Article 37 of the LGPD). Under the Brazilian General Data Protection Law, legitimate interest permits the processing of ordinary personal data without consent, provided that the purposes are lawful, specific, and proportionate, and that such processing does not infringe upon the fundamental rights and freedoms of the data subject. In this respect, the LGPD aligns with the General Data Protection Regulation (GDPR), which also recognizes legitimate interest as a flexible ground for processing. However, while the GDPR requires controllers to conduct and document a balancing test to weigh organizational interests against individual rights, the LGPD goes further by expressly linking legitimate interest to the preparation of a Data Protection Impact Report (Relatório de Impacto à Proteção de Dados Pessoais) whenever the processing may present significant risks. This requirement strengthens the accountability (Teixeira & Guerreiro, 2022: p. 40) framework in Brazil by obliging controllers to justify the necessity of processing and to demonstrate the safeguards adopted. As in the GDPR, legitimate interest under the LGPD cannot be invoked for sensitive personal data, which is subject to stricter conditions and legal bases.

Although the legislator did not determine the minimum content of the record, the LGPD itself provides elements that can be used to define criteria (Teixeira & Guerreiro, 2022: p. 40). These elements include identification of the processing agent and the data subject; nature of the personal data processed; purpose, form, and duration of the processing; information about the shared use of data; legal basis assigned; and information related to the international transfer of personal data (if applicable) (Furtado, 2020: p. 91).

Next, we will conduct a more in-depth analysis of the legal basis applicable to processing personal data for monitoring employees using automated people analytics tools. Next, we will explore the role of the Brazilian National Data Protection Authority (ANPD) in this context.

4.2.1. Consent

According to the LGPD, consent is defined as "the free, informed, and unequivocal expression of agreement by which the data subject consents to the processing of their personal data for a specific purpose" (Art. 5, XII). Therefore, an employee's consent for processing personal data must be given voluntarily and for a specific purpose. Employers must provide information on what data is collected, its intended use, how long it will be stored, who will have access to it, and whether

[16]The law establishes specific deadlines that must be followed. For example, the statute of limitations for filing labor lawsuits is 10 years according to Article 205 of the Civil Code. According to Article 603 of the CLT and Article 19 of Decree No. 3,048/1999, contracts or employee records must be stored indefinitely. According to Article 7, XXIX of the Federal Constitution, the statute of limitations for claims arising from labor relations is five years after the termination of the employment contract.

it will be transmitted to third parties (Doneda, 2006).

An illustrative example in which an employee's consent in the workplace would not be undermined by subordination is the voluntary participation in a corporate wellness program. Suppose a company offers employees the option to join a mindfulness or fitness initiative that involves collecting basic health and lifestyle data through a mobile app. Participation is entirely optional, no employment-related consequences arise from refusal, and the benefits—such as access to gym facilities or wellness workshops—are additional perks rather than conditions of employment. In this context, the employee's decision to consent is genuinely free, as declining would not affect their job security, career progression, or daily work activities, thereby ensuring that the consent is valid and not tainted by the inherent power imbalance of the employment relationship.

Although new legal bases for data processing are available, consent continues to be one of the most frequently used because it can simplify the controller's compliance obligations. When the data subject gives consent, the controller can more easily demonstrate that the processing is lawful, thereby fulfilling the principle of accountability (Teixeira & Guerreiro, 2022: p. 21). However, the scope of consent is limited: it only authorizes the specific controller who obtained it to process the data. If the data is to be shared with third parties, the controller cannot rely on the original consent alone. In such cases, new and explicit consent from the data subject is required—unless another legal basis clearly permits the transfer or disclosure of the data. This limitation underscores the importance of transparency and precision in obtaining consent, as it does not provide a blanket authorization for all forms of data use.

Although consent is recognized as a valid legal basis for processing personal data under the LGPD, in the employment context it is not always the most suitable option. This stems from the inherent power imbalance between employers and employees, where subordination may lead workers to feel that withholding consent could negatively affect their position. As a result, even when consent is formally obtained, it may not be considered truly free or informed, casting doubt on its validity (Bioni, 2019: p. 256). For this reason, in scenarios involving workplace monitoring, other legal bases—such as the employer's legitimate interest or the need to comply with legal obligations—may provide a more appropriate and reliable foundation for processing, while also offering greater protection for employees against potential coercion or misuse of their personal data (Bioni, 2020: pp. 119-120)[17].

Therefore, the choice of legal basis must take into account the specific circum-

[17]The term "free" refers to an action that is spontaneous and not subject to pressure. It is characterized by free will, which is the ability to choose among multiple alternatives. The key issue in determining if consent is truly free is the level of power asymmetry involved. This requires examining the data subject's bargaining power regarding the processing of their personal data. This includes the options available concerning the types of data collected and their potential uses. In short, the "menu of options" offered to the individual calibrates the extent of their consent by helping to balance an otherwise asymmetrical relationship.

stances of each case and the nature of the relationship between the parties. When it comes to sensitive personal data—such as information about health, religion, ethnicity, or sexual orientation—consent is generally the most appropriate basis, as it aligns with the heightened expectations of privacy attached to these categories of data. In such situations, employees must be clearly and transparently informed about the purposes of processing so that their consent is both specific and explicit, in compliance with Article 11, I of the LGPD. This ensures that the use of particularly delicate information is strictly limited to the purposes expressly authorized by the data subject, thereby reinforcing both legal safeguards and the trust necessary for legitimate processing.

4.2.2. Legitimate Interest

Legitimate interest is one of the legal bases for processing personal data under the LGPD. It applies specifically to the processing of ordinary personal data, provided that the controller carries out a balancing test between its own interests (or those of a third party) and the fundamental rights and guarantees of the data subject. Article 10 of the LGPD establishes a four-step test for this assessment. First, it must be verified whether the controller's interest is connected to a legitimate purpose. This purpose cannot conflict with other legal provisions and must be duly justified as necessary for the specific processing of personal data in question (Art. 10, I, LGPD).

Next, determine if the collected data is necessary to achieve the intended purpose (Art. 10, §1, LGPD). Two key questions can guide this step: 1) can the same result be achieved with less data, and 2) could another legal basis justify the processing? If the answer to both is no, proceed to the balancing phase. During the balancing phase, analyze the potential impact of the processing on the data subject and their legitimate expectations (Art. 10, II, LGPD). Determine if the use of the data is consistent with the original purpose. Consider the data subject's expectations and identify any potential negative effects on their autonomy, including the risk of discrimination.

Finally, to process personal data based on legitimate interest, the company must ensure transparency and minimize risks to the data subject. Measures such as data anonymization can mitigate these risks (Art. 10, §§ 2-3, LGPD).

In the context of collecting personal data through employee monitoring for people analytics, employers have a legitimate interest in ensuring that their employees complete their assigned tasks. Using this data to define metrics and identify risks can improve productivity and reduce costs by enabling effective management of workloads and time allocation. This approach ensures that company resources are used appropriately and provides documentation in case of potential litigation. Additionally, it allows organizations to address reports of workplace harassment. When monitoring is conducted with explicit objectives and quantifiable metrics, it can support high-performing employees who might otherwise be overlooked or affected by human bias.

In the case of Sólides, the legitimacy of the employer's interest lies in using behavioral and demographic data (e.g., name, email, telephone number, social security number, and self-declared behavioral tendencies) to create profiles that optimize recruitment and talent management. This aligns with a lawful and organizationally necessary purpose. Regarding necessity, the processing of such ordinary personal data is adequate to achieve the stated goals without resorting to more intrusive or sensitive categories of data. Transparency is ensured when employees are informed that their data will be used to generate behavioral profiles and climate surveys, thereby allowing them to understand the scope of processing. Finally, the impact on rights must be carefully assessed: since the data are not sensitive and are directly provided by the data subject, the risks to privacy and autonomy are relatively low, provided the employer avoids discriminatory or opaque use of the profiling outputs. Taken together, these elements support the viability of legitimate interest as a lawful basis under the LGPD.

For Hubstaff, the legitimate purpose is centered on productivity management in remote or hybrid work arrangements. The company collects ordinary data, such as name, email, position, and user activity information (applications accessed, URLs visited, and time spent on tasks), which are directly connected to performance monitoring. From a necessity perspective, this type of monitoring is limited to operational data that serve to identify workflow bottlenecks and ensure accountability, without extending into unnecessary or sensitive areas. Transparency requires clear disclosure to employees that such activity monitoring will occur and how the resulting reports will be used. As for the impact on rights, the monitoring must be implemented in a proportionate way, ensuring it does not lead to constant surveillance or unreasonable pressure on workers. When the scope of processing is clearly defined, limited to operational data, and subject to oversight, legitimate interest stands as an appropriate legal basis for Hubstaff's processing activities.

By contrast, the practices of WE Controlio, as described in the available documents, suggest that legitimate interest may not be an appropriate legal basis. The company records usernames, email addresses, IP addresses, and browser information, but also engages in far more invasive measures, such as uninterrupted screen recording, access to the content of emails and instant messages, and continuous screenshot capture, often without the employee's awareness. While employers may claim a legitimate purpose in preventing misuse of company resources, the breadth and intensity of this monitoring appear disproportionate to that objective. The lack of transparency and the high degree of intrusion into employees' private communications and activities significantly undermine the balance between organizational interests and fundamental rights. In such a case, legitimate interest would struggle to meet the requirements of necessity and proportionality under the LGPD, making alternative legal bases—such as consent in narrowly tailored circumstances or specific legal obligations—more suitable for legitimizing the processing.

Employers are expected to monitor their employees in the workplace as part of their managerial authority, which is recognized as a legitimate purpose under Brazilian labor law. In some cases, such as Hubstaff, where the monitoring is limited to operational data—like time spent on tasks, applications accessed, and websites visited—the legitimate interest of the employer can serve as a valid legal basis under the LGPD. Here, the collection of ordinary personal data is directly connected to productivity management in remote or hybrid work arrangements, and the monitoring can be proportionate, transparent, and limited to what is necessary to achieve organizational goals.

However, the scope and method of data collection must always remain proportionate and reasonable in relation to the purpose pursued. Sólides, for example, collects personal and behavioral data directly provided by employees in order to generate profiles, climate surveys, and performance indicators. When applied transparently and within well-defined boundaries, this type of people analytics can also be supported by legitimate interest, as the processing involves non-sensitive data and seeks to enhance recruitment and workforce management. By contrast, cases like WE Controlio, which involve constant screen recording, access to emails and instant messages, and uninterrupted screenshots without the employee's awareness, go beyond what is necessary for productivity monitoring. Such practices demonstrate how disproportionate surveillance undermines transparency and fails the balancing test required for legitimate interest to apply.

Finally, even when monitoring falls within managerial prerogatives, legitimate interest cannot serve as a legal basis where the processing involves sensitive personal data. This includes biometric identifiers, health information, and data revealing racial or ethnic origin, religious beliefs, political opinions, or union membership. In such circumstances, the employer must rely on other legal bases under the LGPD—such as the specific and informed consent of the employee or the fulfillment of legal or regulatory obligations—to ensure that the processing is lawful.

4.2.3. Compliance with Legal or Regulatory Obligations by the Controller

The controller may use this legal basis to comply with legal or regulatory obligations when applicable legislation or regulations require monitoring as a legal obligation. Examples of such cases include workplace safety issues, protection of confidential information, and compliance with specific standards for certain professions. Employers are not required to obtain their employees' consent for processing their personal data in such cases. However, employers must clearly communicate the circumstances under which employee data will be processed in accordance with the transparency principle (Teixeira & Guerreiro, 2022: p. 21).

In this sense, companies like Mywork illustrate how compliance with legal obligations may serve as a legal basis for processing. Mywork collects information regarding employees' entry and exit times through geolocation and photo registration. Under Brazilian labor law, employers with more than twenty employees must keep accurate records of working hours. The use of digital tools such as Mywork's time and attendance system directly responds to this legal requirement.

In such cases, the employer is not relying on legitimate interest or consent, but rather on the need to comply with Article 74 of the CLT, which establishes the duty to record employees' working hours. The data processed is therefore justified by law and limited to what is necessary for compliance.

Similarly, Factorial offers attendance and absence management services, including webcam monitoring and the collection of entry and exit times. When these services are used exclusively to meet the employer's obligation to document employees' working hours, the processing of personal data falls under the legal obligation basis rather than legitimate interest. The decisive factor is whether the monitoring is restricted to fulfilling the statutory duty to maintain time records, as opposed to broader, discretionary purposes such as performance evaluation. By grounding the processing in legal obligation, employers both comply with labor law and respect the principle of necessity under the LGPD, ensuring that only data strictly required by the regulation are collected and processed.

For employees covered by the CLT, Article 6 establishes that employers may use work supervision measures. However, Article 74 stipulates that companies with more than 20 employees must maintain a manual, mechanical, or electronic record of their employees' arrival and departure times. Based on this legal basis, such devices could justify the processing of personal data for monitoring purposes.

4.2.4. Contract Performance

The legal basis for executing a contract establishes that personal data may be processed when necessary to fulfill the agreed-upon contractual terms or preliminary procedures related to a contract involving the data subject, at the data subject's request. Therefore, if collecting and processing personal data is essential to performing an employment contract, the contracting company may proceed without obtaining the data subject's explicit consent. However, the collection and processing of personal data must be strictly limited to fulfilling the contract or pre-contractual obligations, and it cannot be used for any other purpose.

For instance, Time Doctor collects information such as employee names, emails, and activity records (including time spent on each task, applications used, and websites visited) to generate productivity reports. When an employee's contract explicitly requires compliance with working hours, task monitoring, or performance evaluations tied to deliverables, the processing of such data is directly linked to fulfilling contractual obligations. In this context, the company does not need to rely on consent or legitimate interest, since the monitoring is necessary to perform the terms of the employment contract itself. The key limitation, however, is that the data collected must remain proportional to the contractual purpose and not be extended to unrelated forms of surveillance.

Similarly, Mywork manages attendance records by collecting employees' personal data such as full name, personal documents (e.g., RG, CPF, Work Permit), date of birth, and geolocation data at the time of entry and exit. This information is essential to enforce the contractual terms related to working hours, overtime calculation, and payroll management. In this context, processing is grounded on

the contractual basis, as the employer must ensure accurate compliance with the agreed-upon work schedule and related obligations. However, if the company were to expand the use of geolocation data to monitor employees outside the scope of contractual duties—such as tracking their movements beyond working hours—such processing would no longer fall within contract performance and would require a different legal basis under the LGPD.

Note that, as with the legal basis of legitimate interest, performance of a contract cannot justify processing sensitive data. Therefore, it is not possible to classify the processing of biometric data, health data, or data revealing racial or ethnic origin, religious beliefs, political opinions, union membership, or membership in religious, philosophical, or political organizations under the legal basis of contract performance.

4.3. The Role of the National Data Protection Authority (ANPD) in Guaranteeing the Rights of Personal Data Subjects

To monitor employees using people analytics, it is necessary to analyze the role of the National Data Protection Authority (ANPD) in processing personal data. The ANPD is a special autonomous agency affiliated with the Ministry of Justice and Public Security (Decree No. 11,758, 2023). It is responsible for ensuring the security of personal data and supervising the application, regulation, and enforcement of the LGPD in Brazil (Autoridade Nacional de Proteção de Dados, 2023). Therefore, the ANPD is a key component in ensuring the efficacy of the LGPD for both data processors and data subjects (Bioni, 2020).

According to Article 20 of the LGPD, data subjects have the right to request a review of decisions based solely on automated processing of personal data that affect their interests. This includes decisions intended to define their professional profile. Therefore, employers are responsible for providing employees with clear and adequate information regarding the criteria and procedures used in automated decisions within the scope of people analytics, while observing commercial and industrial secrets (§1). If such information is not provided, the ANPD reserves the right to conduct an audit to verify any discriminatory aspects in the automated processing of personal data.

This provision underscores the ANPD's subsidiary role in this situation. If the controller refuses to provide a detailed report on the criteria and procedures used for the automated decision, the Authority may audit it to verify possible discriminatory aspects and confirm that the data processing complies with the law and the fundamental rights established in the Constitution.

Furthermore, the ANPD may establish specific guidelines and regulations for the collection, processing, and storage of personal data in the context of employee monitoring using artificial intelligence (Information Commissioner's Office, 2023)[18]. The ANPD may penalize organizations that fail to comply with the legis-

[18]In October 2023, the Information Commissioner's Office (ICO) published guidelines to ensure lawful monitoring in the workplace. These guidelines are in line with the European General Data Protection Regulation (GDPR).

lation. These penalties may include warnings, fines[19], and suspension or prohibition from activities involving the processing of personal data.

It is important to note that the LGPD, enacted in 2018, is based on the European General Data Protection Regulation (GDPR), which was enacted in 2016. Consequently, many of the powers granted to the ANPD are also granted to European data protection authorities. These authorities have a more consolidated role, so analyzing them will help us understand how the ANPD may position itself in the future.

The General Data Protection Regulation (GDPR) stipulates that European data protection authorities are responsible for enforcing the law to protect the fundamental rights and freedoms of natural persons with regard to the processing of personal data and to facilitate the free flow of personal data within the Union (Article 51 of the GDPR). Furthermore, all authorities from the European Data Protection Board (EDPB) collaborate to ensure enforcement at the national and cross-border levels (Europa.eu, 2022).

To gain insight into how European authorities have addressed the issue of personal data processing for employee monitoring purposes, a search was conducted for decisions on the subject since the law was enacted (2016). The research was conducted on the Enforcement Tracker platform (Enforcement Tracker, 2023) using the following keywords: Please use the terms "employee monitoring," "employee," and "working environment." A total of 268 decisions were identified, of which eight specifically address the issue of employee monitoring by companies.

Table 6 below provides an overview of the sanctions imposed by European data protection authorities and their respective justifications.

As illustrated in **Table 6**, companies are primarily found guilty of collecting personal data from their employees through monitoring that fails to comply with general data processing principles, such as necessity, transparency, and accountability. Furthermore, in Europe, punitive measures are becoming increasingly common, with the imposition of heavy fines.

The GDPR explicitly establishes what a company can and cannot do with employee data, restricting the use of personal data for automated scoring and employee profiling purposes. Additionally, data subjects cannot be subject to automated decisions unless they fall under one of the exceptions provided for in the regulation (Souza, Perrone, & Magrani, 2021). In contrast, the LGPD offers greater flexibility than the European regime by not prohibiting the execution of automated decisions. Rather, it establishes safeguards and duties for data processors to fol-

[19]In July 2023, the ANPD issued its first penalty for a violation of the LGPD. The penalty was issued to the micro telemarketing company Telekall Inforservice for failing to: i) prove the application of legal bases to the processing of personal data, ii) record its data processing activities, iii) submit the Data Protection Impact Report to the Authority, iv) appoint a personal data officer, and v) comply with the ANPD's request. For more information, see: Autoridade Nacional de Proteção de Dados. (2023, July). ANPD aplica a primeira multa por descumprimento à LGPD. Retrieved August 5, 2025, from https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-aplica-a-primeira-multa-por-descumprimento-a-lgpd.

low, including the right of review set out in Article 20.

In Brazil, the Judiciary has the authority to impose sanctions on companies that mishandle their employees' personal data. However, as the ANPD's actions align with a global movement by data protection authorities to establish remedial or preventive measures to ensure compliance with privacy and data protection standards by public and private entities worldwide, this scenario may evolve, potentially leading to the ANPD playing a more active role in cases involving the processing of Brazilian workers' personal data. In this context, it remains to be seen whether the Brazilian authority will follow the European trend of imposing fines and increasing the amounts considered for fines.

Table 6. Decisions by European data protection authorities on real-time monitoring of employees (Source: Elaborated by the authors).

Decision Number (CMS Law)	Date of Judgment	Responsible Authority	Violation Committed	Penalty Applied	Justification
ETid-257	02/08/2019	Hungarian National Authority for Data Protection and Freedom of Information (NAIH)	Monitoring through closed-circuit television cameras, in non-compliance with the applicable legal basis.	Fine of €4290	Non-compliance with the general principles of data processing
ETid-259	15/10/2019	Hungarian National Authority for Data Protection and Freedom of Information (NAIH)	Monitoring of an employee's desktop, laptop, and emails while on medical leave by the employer, without their knowledge, in order to ensure that their tasks were performed by other employees.	Fine of €2860	Non-compliance with the general principles of data processing
ETid-1107	09/03/2022	Hellenic Data Protection Authority (HDPA)	An employee objected to the continuous monitoring of their online training courses offered via video call, but the employer continued the monitoring without a sufficient legal basis for data processing.	Fine of €2000	Insufficient compliance with data subjects' right
ETid-710	07/06/2022	Spanish Data Protection Agency (AEPD)	Excessive monitoring. Installation of numerous video cameras on the company premises, including in break areas.	Fine of €19,600	Non-compliance with the general principles of data processing

Continued

ETid-1723	2022	Data Protection Authority of Bremen (Germany)	Installation of a GPS system in the company car for monitoring purposes. It was found that data processing occurred beyond working hours and for purposes other than those originally intended.	Fine in a five-digit amount	Non-compliance with the general principles of data processing
ETid-1699	23/03/2023	Romanian National Supervisory Authority for Personal Data Processing (ANSPDCP)	Installation of a GPS system in the company car for monitoring purposes without providing clear information to employees. It was found that data processing occurred beyond working hours and for purposes other than those originally intended.	Fine of €5000	Non-compliance with the general principles of data processing
ETid-1749	07/04/2023	Romanian National Supervisory Authority for Personal Data Processing (ANSPDCP)	Use of video surveillance cameras on company premises to monitor people's access and ensure the security of facilities and property, carried out without employees' consent and beyond the intended purpose.	Fine of €3000	Non-compliance with the general principles of data processing
ETid-1994	01/06/2023	Italian Data Protection Authority (Garante)	Excessive video monitoring with real-time image recording and audio recordings, and the use of an application to continuously track employees' location via GPS, without their knowledge.	Fine of €20,000	Non-compliance with the general principles of data processing

In light of the cases analyzed, our perception is that many of the companies operating in Brazil could significantly improve the quality of the information they provide about how employees' personal data are processed, as well as their compliance with the principles and rules established by the LGPD. Transparency, proportionality, and accountability often appear insufficiently addressed in the materials and practices disclosed, which creates uncertainty for data subjects and may expose employers to legal risks.

Looking ahead, it is expected that the ANPD will strengthen its institutional

capacity in the coming years to guide and, when necessary, sanction organizations, thereby fostering a culture of compliance more closely aligned with international standards and ensuring greater protection of Brazilian workers' personal data. To enhance the practical implications of this study, it is important to consider future guidelines that the ANPD could issue to clarify the limits of employee monitoring. The Authority could, for example, develop model clauses for employment contracts that address data collection in a transparent manner, or establish specific guidelines for conducting Data Protection Impact Assessments (DPIAs) on monitoring technologies. Such initiatives would provide legal certainty for both employers and employees, aligning market practices with the fundamental principles of the LGPD.

5. Conclusion

In light of the cases analyzed, our perception is that many of the companies operating in Brazil could significantly improve the quality of the information they provide about how employees' personal data are processed, as well as their compliance with the principles and rules established by the LGPD. Transparency, proportionality, and accountability often appear insufficiently addressed in the materials and practices disclosed, which creates uncertainty for data subjects and may expose employers to legal risks.

Employee monitoring is a legitimate requirement for employers and an expectation for those being monitored, serving as a management and risk control measure. While not a new concept, integrating artificial intelligence significantly increases the capacity to process personal data and evaluate employee performance. In the current business environment, the number of HR tech professionals specializing in people analytics is growing.

However, automated decision-making processes carry inherent risks, such as potential discrimination and a lack of transparency. In this regard, monitoring should be kept to a minimum and should not amount to unprecedented surveillance. There are two scenarios in which such surveillance can occur: first, when the employer collects data that goes beyond the work environment, and second, when detailed information about employees' use of time is collected so accurately that it compromises their autonomy in performing their assigned tasks.

Since this is a recent development, there are no explicit rules about what is and isn't allowed. This makes it necessary to read the existing rules. In this context, Brazilian law—specifically the LGPD—establishes limits and obligations to ensure privacy in the workplace. The law addresses critical issues, such as safeguarding the fundamental right to privacy and intimacy, establishing legal grounds for processing personal data, setting data retention periods, and ensuring that employees are provided clear information. HR Techs and the companies that hire them must take all these provisions into account when monitoring their employees.

The ANPD is well-positioned to fulfill a pivotal role in the regulation and supervision of these practices, conducting audits to verify the potential for discrim-

inatory aspects in the automated processing of personal data. Additionally, the ANPD is responsible for establishing specific guidelines and regulations to guide companies' practices, ensuring that data processing is carried out in an ethical and legal manner. The evolution of this scenario will depend on the ANPD's ability to become more active in cases involving the processing of Brazilian workers' personal data, possibly increasing the amounts of fines, following the European example.

In order to mitigate legal and ethical risks, employers should adopt a "best practices" approach. Firstly, it is essential to limit the purpose of monitoring and ensure that it is carried out for a legitimate and specific purpose. Secondly, it is crucial to minimize data collection, ensuring that only the strictly necessary information is gathered for the specific purpose. It is essential to be transparent with employees regarding the data collected and the reasons behind it, in order to build trust and comply with legal obligations. Finally, when using legitimate interest as a legal basis, it is essential to perform a balancing test to ensure that the interests of the company are balanced with the rights and freedoms of employees.

In conclusion, this paper addressed the risks and challenges that emerge from this practice, particularly with regard to privacy protection and regulatory compliance. Consequently, ongoing research is imperative to ensure that the implementation of AI for employee monitoring in Brazilian companies is mutually beneficial, respecting privacy and ethics.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

ActivTrak (2024). *ActivTrak Privacy Statement*. https://www.activtrak.com/privacy-policy/

Ajunwa, I. (2023). *The Quantified Worker: Law and Technology in the Modern Workplace*. Cambridge University Press. https://doi.org/10.1017/9781316888681

Aloisi, A., & De Stefano, V. (2022). Essential Jobs, Remote Work and Digital Surveillance: Addressing the COVID-19 Pandemic Panopticon. *International Labour Review, 161,* 289-314. https://doi.org/10.1111/ilr.12219

Arbex, G. (2020). Exclusive: Study Maps Brazil's HR Techs and Highlights Huge Growth Potential. *Forbes*. https://forbes.com.br/forbes-tech/2020/06/exclusivo-estudo-mapeia-rh-techs-do-brasil-e-aponta-enorme-potencial-de-crescimento/

Ashworth, B. (2023). *Amazon Watches Its Workers and Waits for Them to Fail*. WIRED. https://www.wired.com/story/amazon-worker-tracking-details-revealed/

Autoridade Nacional de Proteção de Dados (2023). *ANPD Applies First Fine for Non-Compliance with the LGPD*. National Data Protection Authority. https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-aplica-a-primeira-multa-por-descumprimento-a-lgpd

Ball, K. (2021). *Electronic Monitoring and Surveillance in the Workplace: Literature Review and Policy Recommendations*. European Commission.

Bar-Gil, O., Ron, T., & Czerniak, O. (2024). AI for the People? Embedding AI Ethics in HR and People Analytics Projects. *Technology in Society, 77,* Article ID: 102527. https://doi.org/10.1016/j.techsoc.2024.102527

Bioni, B. (2020). *Tratado de Proteção de Dados Pessoais*. Gen Group.

Bioni, B. R. (2019). *Proteção de dados pessoais: A função e os limites do consentimento*. Gen Publishing.

Bodie, M. T., Cherry, M. A., McCormick, M. L., & Tang, J. (2017). The Law and Policy of People Analytics. *The University of Colorado Law Review, 88,* 961.

Braverman, H. (1987). *Labor and Monopoly Capital: The Degradation of Work in the Twentieth Century*. Guanabara.

Brazil (1943). *Decree-Law No. 5,452, May 1, 1943*. https://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm

Brazil (1988). *Constitution of the Federative Republic of Brazil of 1988*. Federal Senate. http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm

Brazil (2018). *Law No. 13,709, August 14, 2018*. Official Gazette of the Federative Republic of Brazil. http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm

Brewer, N. (1995). The Effects of Monitoring Individual and Group Performance on the Distribution of Effort across Tasks. *Journal of Applied Social Psychology, 25,* 760-777. https://doi.org/10.1111/j.1559-1816.1995.tb01774.x

Capterra (2022). *Do Companies in Brazil Already Monitor Employees?* https://www.capterra.com.br/blog/2712/monitoramento-funcionarios

Clever Control (2023). *Privacy Policy*. https://clevercontrol.com/pt/privacy-policy/

Controlio (2023). *Controlio: Cloud-Based Computer Monitoring Software*. https://controlio.net/

de Brito, A. P. (2024). People Analytics and the COVID-19 Pandemic: How Empathy and Privacy Turned out the Hot Topics. In M. J. Sousa et al. (Eds.), *Incorporating AI Technology in the Service Sector: Innovations in Creating Knowledge, Improving Efficiency, and Elevating Quality of Life* (pp. 189-213). Apple Academic Press. https://doi.org/10.1201/9781003378068-9

Dias, M. (2019). *People Analytics: What It Is, Benefits and How to Apply It in HR*. Gupy.io. https://www.gupy.io/blog/people-analytics#Cp1

Doneda, D. (2006). *From Privacy to Data Protection*. Renovar.

Ekka, S. (2021). HR Analytics: Why It Matters. *Journal of Contemporary Issues in Business and Government, 27,* 2283-2291.

Ekran System (2023). *Insider Threat Protection Software*. https://www.ekransystem.com/en

Enforcement Tracker (2023). *GDPR Enforcement Tracker-List of GDPR Fines*. https://www.enforcementtracker.com/

Eurofound (2020). *Employee Monitoring and Surveillance: The Challenges of Digitalisation.* Publications Office of the European Union, Luxembourg. https://www.eurofound.europa.eu/en/publications/all/employee-monitoring-and-surveillance-challenges-digitalisation

Europa.eu (2022). *EDPB Chairmanship*. European Data Protection Board. https://edpb.europa.eu/about-edpb/who-we-are/edpb-chairmanship_en

Fabro, C. (2022). *Bossware: How Programs Spy on Employees without Their Knowledge*. TechTudo. https://www.techtudo.com.br/noticias/2022/06/bossware-como-funciona-programa-

que-vigia-funcionarios-sem-que-eles-saibam.ghtml

Factorial (2024). *Privacy at Factorial*. https://factorialhr.com.br/politica-privacidade

FocusRO (2023). *FocusRO: ML-Based Automated Employee Productivity & Time Tracking Software*. https://focusro.com/

fSense (2023). *fSense Is Your Complete Ally for Managing Your Teams' Productivity*. https://fsense.com/pt/

Furtado, T. N. (2020). Recording Personal Data Processing Operations-Data Mapping/Data Discovery: Why It's Important and How to Conduct It. In O. Blum, R. Vainzof, & H. F. Moraes (Eds.), *Data Protection Officer-Theory and Practice under LGPD and GDPR* (pp. 91, 98). Thomson Reuters Brasil.

Giuntini, A., Sylvia da Fonseca, A., Coelho, P. et al. (2021). *LGPD in Labor Relations*. https://oabdf.org.br/wp-content/uploads/2021/08/eBook_LGPD-nas-Relacoes-de-Trabalho-1-1.pdf

Hubstaff (2023). *Hubstaff Privacy Policy*. https://hubstaff.com/privacy

Information Commissioner's Office (2023). *ICO Publishes Guidance to Ensure Lawful Monitoring in the Workplace*. https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/10/ico-publishes-guidance-to-ensure-lawful-monitoring-in-the-workplace

InterGuard (2023). *Privacy Policy*. InterGuard-Employee Monitoring & Productivity Tracking. https://www.interguardsoftware.com/privacy-policy/

Kickidler (2023). *Program to Monitor and Control Employee Computers*. https://www.kickidler.com/br/

Larson, J. R., & Callahan, C. (1990). Performance Monitoring: How It Affects Work Productivity. *Journal of Applied Psychology, 75,* 530-538. https://doi.org/10.1037/0021-9010.75.5.530

LinkedIn Talent Solutions (2023). *Global Talent Trends*. LinkedIn. https://business.linkedin.com/talent-solutions/global-talent-trends?trk=bl-po_global-talent-trends-2020

Lloyd, J. (2006). Management Email Monitoring Brings Big Brother to Mind. *Receivables Report for Americas Health Care Financial Managers, 21,* 6-7.

Magalhães, T. (2025). *Minimum Wage in São Paulo: What It Is and Who Is Eligible*. Solides Blog. https://solides.com.br/blog/salario-minimo-em-sao-paulo/

Maria, L. (2017). Monitoring Emails and Websites, Employee Privacy and Employer Control Power: Scope and Limitations. *Revista Jurídica Cesumar-Mestrado, 5,* 115-130.

Marques, L. (2022). *"Bossware": Programs Monitor Employees without Their Noticing*. UOL. https://www.uol.com.br/tilt/noticias/redacao/2022/04/28/bossware-empresas-monitoram-funcionarios-sem-que-eles-percebam.htm

McCartney, S., & Fu, N. (2022). Promise versus Reality: A Systematic Review of the Ongoing Debates in People Analytics. *Journal of Organizational Effectiveness: People and Performance, 9,* 281-311. https://doi.org/10.1108/joepp-01-2021-0013

Monitask (2023). *Privacy Policy*. https://www.monitask.com/pt/home/privacypolicy

Monitoo (2023). *Employee Monitoring Software*. https://monitoo.com.br/

Morgan, K. (2023). *How Worker Surveillance Is Backfiring on Employers*. BBC. https://www.bbc.com/worklife/article/20230127-how-worker-surveillance-is-backfiring-on-employers

Mywork (2023). *Privacy at Mywork*. https://www.mywork.com.br/politica-de-privacidade

Pan American Health Organization (2023). *History of the COVID-19 Pandemic*.

https://www.paho.org/pt/covid19/historico-da-pandemia-covid-19

Pestana, M. (2020). *The Principles in Data Processing under the LGPD (General Data Protection Law)*. https://www.conjur.com.br/2020-mai-25/marcio-pestana-principios-tratamento-dados-lgpd/

Pombo, B. (2023). *Labour Court Condemns Companies under the LGPD*. Valor Econômico. https://valor.globo.com/legislacao/noticia/2023/03/13/justica-do-trabalho-condena-empresas-com-base-na-lgpd.ghtml

Privacy Affairs (2023). *Employee Monitoring Technology Explained*. https://www.privacyaffairs.com/employee-monitoring/

Ribeiro, A. de F. (2015). Taylorism, Fordism and Toyotism. *Lutas Sociais, 19,* 65-79.

Ribitzky, R. (2023). *Active Monitoring of Employees Rises to 78%*. ABC News. https://abcnews.go.com/Business/story?id=88319&page=1

Segalla, A. (2021). *How Companies Are Monitoring Employees Working from Home*. VEJA. https://veja.abril.com.br/economia/como-as-empresas-estao-monitorando-os-funcionarios-no-home-office/

Shrikant, A. (2023). *Companies Use AI to Monitor Workers—45% of Employees Say It Has a Negative Effect on Their Mental Health*. CNBC. https://www.cnbc.com/2023/09/08/employers-using-ai-to-monitor-workers-has-negative-impact-on-employees.html

Sólides (2023). *Privacy Policy*. https://solides.com.br/politica-de-privacidade/

Souza, C. A., Perrone, C., & Magrani, E. (2021). The Right to Explanation between European Experience and Its Formalization in the LGPD. In D. Doneda et al. (Eds.), *Treaty on Personal Data Protection* (pp. 243-270). Forense.

Taylor, F. W. (1947). *Scientific Management, Comprising Shop Management*. Harper.

Teixeira, T., & Guerreiro, R. M. (2022). *General Personal Data Protection Law (LGPD): Article-by-Article Commentary*. Saraiva Publishing.

Teramind (2023). *Endpoint User Activity Monitoring Software*. https://www.visier.com/lp/age-of-people-analytics-research-report/

Time Doctor (2023). *Privacy Policy*. https://www.timedoctor.com/privacy_policy

Visier (2018). *The Age of People Analytics Research Report*. https://www.visier.com/lp/age-of-people-analytics-research-report/

West, D. M. (2021). *How Employers Use Technology to Surveil Employees*. Brookings. https://www.brookings.edu/blog/techtank/2021/01/05/how-employers-use-technology-to-surveil-employees/

Zanatta, P., & Brotero, M. (2023). *Hybrid Work Model Is Used by 56% of Companies in Brazil, Says Study*. CNN Brasil. https://www.cnnbrasil.com.br/economia/modelo-de-trabalho-hibrido-e-usado-por-56-das-empresas-no-brasil-diz-estudo/

Ziegler, B. (2023). Should Companies Track Workers with Monitoring Technology? *Wall Street Journal*. https://www.wsj.com/articles/companies-track-workers-technology-11660935634?mod=djemCybersecruityPro&tpl=cy