Digital Privacy in Smart Work Environments: Between the Challenges of Electronic Monitoring and the Protection of Professional Rights in the Age of Artificial Intelligence

Benguettat Khadidja
Abdelhamid Ibn Badis University, International Law for Development Laboratory Mostaganem (Algeria), *Khadidja.benguettat@univ-mosta.dz*

Received: 25/02/2026 *Accepted: 02/06/2026* *Published: 31/07/2026*

Abstract:

Work environments have been profoundly transformed by artificial intelligence and digital technologies, enabling extensive data collection and enhanced productivity. However, these advancements raise significant concerns regarding the protection of employees' digital privacy. This study examines French legislation as a leading regulatory model, with references to Algerian law to highlight legislative gaps. It analyzes how digital monitoring and data analytics may infringe privacy if not governed by strict safeguards. The research emphasizes workers' rights to object to data processing, access their data, and request corrections. It stresses the need to balance technological innovation with fundamental rights. The study also calls for transparent policies on automated data processing and clear institutional accountability. Ultimately, it concludes that smart digital monitoring requires a comprehensive legal framework aligned with technological progress while safeguarding workers' rights.

Keywords *: Digital privacy; Artificial intelligence; Personal data;Smart work environment.*

1. INTRODUCTION

Work environments have witnessed profound transformations over recent decades as a result of rapid technological advancements, particularly the widespread adoption of artificial intelligence and smart digital technologies, which have significantly changed the nature of work and its traditional practices. The ability to gather and process vast amounts of data associated with professionals has contributed to increased productivity and improved performance. However, it has simultaneously raised serious

concerns concerning the protection of digital privacy and professional rights.

The significance of this study lies in the fact that digital privacy constitutes a crucial right for professionals, recognized within the framework of international human rights law, and is directly associated with work efficiency as well as the psychological well-being of individuals in the workplace. The growing reliance on electronic monitoring and artificial intelligence systems requires a careful and balanced examination of technological innovation on the one hand, and the safeguarding of personal data and the protection of professional rights on the other.

In this context, and given that Algerian legislation remains in a developmental stage with regard to regulating the protection of personal data in digital work environments, and that its practical enforcement mechanisms have not yet reached a sufficient level of maturity, this study mainly draws on the French experience. This choice is justified by the advanced institutional and legislative framework of the French legal system, particularly following the adoption of the General Data Protection Regulation. This framework allows the research problem statement to be explored through a more comprehensive and mature model, while also offering insights that may be adapted to the Algerian reality.

Therefore, the problem statement addressed in this study is as follows: How can digital privacy and professional rights be ensured in smart work environments in light of the challenges posed by electronic monitoring and the integration of artificial intelligence, and to what extent do economic institutions comply with international data protection laws?

Accordingly, this study aims to analyze the balance between technological innovation and the protection of personal data in smart work environments, to determine the challenges related to electronic monitoring and their effect on professional rights, and to evaluate the extent to which economic institutions comply with relevant international standards and legal frameworks. To achieve these objectives, a legal-analytical methodology is adopted to examine international and comparative legal

frameworks, especially French legislation alongside a comparative approach to assess different regulatory experiences, and an inductive method to identify the practical risks related to the digitization of work environments.

The study is devided into two main chapters. The first chapter addresses digital privacy in smart work environments between innovation and the protection of rights, while the second examines the legal risks related to electronic monitoring and the extent of institutional compliance with privacy laws.

2. Artificial Intelligence and Smart Work Environments: Between Digital Data and Privacy Protection Requirements

The world of work is experiencing rapid transformation due to the integration of artificial intelligence technologies, which now structure multiple aspects of smart work environments. This development has resulted in the appearance of massive digital data that is processed and used in human resource management, making it necessary to understand both the nature of these technologies and the data they generate. As a result, there is a pressing need to study artificial intelligence, smart work environments, and personal data as a foundation for understanding their effect on workers' privacy.

2.1. Conceptual Framework of the Study

The use of artificial intelligence in modern organizations has become an undeniable reality, particularly in light of the growing reliance on personal data in managing human resources. Smart work environments promote efficiency but simultaneously create a complex digital space where technology intersects with fundamental workers' rights.

2.1.1. The Concept of Artificial Intelligence

Artificial intelligence is regarded as one of the branches of computer science and a cornerstone of the technology industry in the current era. Notably, the term "Artificial Intelligence" was first coined by American computer scientist John McCarthy in 1956, who defined it as "the science of engineering intelligent machines (HAI, 2020)."

Artificial intelligence (AI) is generally described as "the ability to fulfill human-level performance in all cognitive tasks, such that the human

mind cannot distinguish between human and machine behavior. (Hallevy, 2013, p. 2)" Broadly, it refers to the capacity of digital machines and computers to perform specific tasks that simulate those conducted by intelligent living beings, such as the ability to think, learn from past experiences, or engage in other processes requiring mental operations (Saidani Faiza, 2022, p. 414).

From a legal standpoint, legislative frameworks have varied in providing a comprehensive definition of artificial intelligence, due to its unique features and the differing levels of technological advancement across countries. This has emphasized the need for specific legal regulation. This study adopts the definition provided by the European Parliament, which describes AI as "any tool utilized by a machine to reproduce behaviors related to humans, such as thinking, planning, and creativity. (European Parliament Resolution, 2017)"

Similarly, the French National Commission on Informatics and Liberties defines artificial intelligence as "a logical and automated process, generally grounded in algorithms, capable of performing well-defined tasks. (CNIL)"

2.1.2. The Concept of Personal Data

Personal data has been defined in the legislation of most countries. This subsection introduces its definition according to Algerian and French law.

The Algerian legislator defines personal data in Law No. 18-07, concerning the protection of natural persons in the processing of personal data (Law No. 18-07, 2018). Article 3/1, drawing on international conventions, defines personal data as: "any information, regardless of its form, relating to an identified or identifiable person, directly or indirectly, particularly by reference to an identification number or to one or more components specific to their physical, physiological, genetic, biometric, psychological, economic, cultural, or social identity."

In French law, legislation is closely influenced by European Union regulations (Europe, 1981). The EU defines personal data in the Convention

on the Protection of Individuals with regard to the Automatic Processing of Personal Data (Article 2(1): "Personal data" means any information relating to an identified or identifiable natural person Convention 108).

Nevertheless, the French legislator preceded the EU by enacting Law No. 78-17 on Information, Files, and Liberties, which defines personal data in Article 2 as: "any information relating to a natural person who is identified or identifiable, directly or indirectly, by reference to an identification number or to one or more elements specific to their identity, considering all the means likely to enable their identification."

From these definitions, numerous conclusions can be drawn:

- The protected person under both legislations is a natural person, which excludes legal person.
- The data either identifies the person or makes him identifiable.
- The Algerian legislator provides a broader and more detailed specification of the components that define personal data, whereas French legislation is more concise.

Concerning an employee's personal data, it can be referred to as: "any information relating to an identified or identifiable employee that may concern his identity, professional life, or behavior within or outside the work environment, collected or processed by the employer or his representatives in the context of the employment relationship."

Such data may include, for example:

- Name, address, phone number, salary, social security number, etc.;
- Attendance and departure records, performance evaluations, etc.;
- Health or psychological information associated with work;
- Photographs and audio or video recordings;
- Behavioral analyses derived from artificial intelligence technologies.

2.1.3. The Concept of Smart Work Environments

The concept of a smart workplace or work environment forms part of the broader notion of the "modern workplace." Due to the novelty of the concept and its rapid evolution driven by digital transformation, there is no single, universally accepted definition of a "smart work environment."

According to the International Labour Organization, while there is no precise definition, the emphasis is placed on balancing innovation with the protection of fundamental right. For instance, the ILO's 2019 report *"Work*

for a Brighter Future" addresses *"digitalization and technological transformation"* and their effect on the work environment.

In the same context, ILO Recommendation No. 195 of 2004 on human resource development encourages and facilitates the use of information and communication technologies in the workplace (International Labour Conference, 2004).

Despite the absence of a unified definition, a smart work environment can be defined as *"a technology-enabled environment that promotes productivity, efficiency, and employee collaboration. It leverages advanced technologies, such as the Internet of Things, artificial intelligence, and data analytics, to automate tasks, streamline processes, and create a connected workspace.* (Ritika, 2024)*"*

A smart work environment is a professional setting that relies on modern technologies, intelligent systems, employee-centered design, and data-driven insights to create a flexible work environment that adapts to different work patterns and needs. Its primary purpose is to enhance productivity, promote communication, and offer greater flexibility in task execution (Miro Miroslavov, 2024).

Hence, smart work environments are distinguished by the following characteristics:

- Using smart systems such as the Internet of Things, artificial intelligence, cloud computing, big data, and collaborative digital solutions.
- Relying on data analysis to support decision-making through performance monitoring (tasks completed, time spent, etc.), anticipating organizational needs, and optimizing resources (e.g., electricity consumption).
- Supporting hybrid work models that combine in-person and remote work, often grounded in personal preference or job requirements. This model is increasingly adopted, particularly in technology companies.

2.2. The Impact of Artificial Intelligence on Employee Privacy in the Workplace

The integration of artificial intelligence in the work environment has led to the emergence of a new form of employee subordination, grounded in monitoring professional activity rather than the individual, often through concealed technological means that may be activated without the employee's knowledge.

2.2.1. Technological Monitoring of Employee Behaviour and Movements

This is typically conducted using magnetized electronic cards or surveillance cameras.

2.2.1.1. : Magnetized Electronic Cards

Employers often rely on magnetized cards to track employee attendance and departure. These cards include the employee's personal information and are electronically linked to the human resources department. When the card is swiped through the designated device, the employee's entry and exit times are automatically recorded, allowing precise tracking of their movements within the institution.

The use of electronic cards to monitor employee movements raises two main issues:

- **Employee Freedom of Movement within the Institution**

Once an employee signs an employment contract, they implicitly agree to comply with the employer's rules concerning access and movement within the workplace. While this is regarded as an exercise of the employer's authority to organize work, the expansion of modern technology raises concerns that such authority may exceed its limits, potentially infringing on employee privacy (Al-Ahwani, 1987, p. 167).

Since the employer issues the card, the electronic data stored on it can constitute a digital file for the employee, giving the employer direct access to all information without needing explicit consent (Khelaf, 2010-2011, p. 83).

One of the most significant issues raised by the use of electronic cards in the workplace is the potential restriction of the employee's freedom of movement, a fundamental liberty. As a general principle, individual

freedoms within the organization should remain exceptional and justified only by security or production-related oversight. The employer's authority to use such cards should be proportionate to the intended purpose (Lefebvre, 1998, p. 131). However, in many institutions that apply electronic card systems, such justifications are often lacking. This raises concerns associated with freedom of movement, particularly for employee representatives or union delegates, as freedom of movement within the institution is generally recognized. Accordingly, it becomes necessary to strike a balance between the employer's interest in preventing theft or securing sensitive areas and the rights of employee representatives to perform their duties (Diab, 2001, p. 110).

- **Protection of Personal Information on the Electronic Card**

The electronic card operates as a personal information system. It identifies the holder, allows for electronic signatures, stores data securely, and can track the employee's movements and behaviour, including the time and location of specific actions (Lyon-Caen, 1992, p. 144).

2.2.1.2. Surveillance Cameras for Monitoring Employee Movements: Between Support and Opposition

Opinions differ concerning the legality of employer monitoring through cameras, with both supporting and opposing viewpoints:

- **Support for Monitoring via Cameras**

Some legal scholars assert that video surveillance is more effective than traditional human monitoring performed by the employer, as cameras record and store all information about employee movements across time and location (Qassem, 2011, p. 146).

- **Opposition to Monitoring via Cameras**

Others view camera surveillance of employees unlawful, as cameras inherently constitute a form of monitoring that is disproportionate to the intended purpose.

Critics also argue that such monitoring infringes on individual's personal autonomy. Furthermore, surveillance cameras may represent an inappropriate means, going beyond the objective the employer aims to

fulfill and giving rise to issues unrelated to the professional sphere, but rather impacting the individual's personality and private self, such as the installation of cameras in changing rooms (Grévy, 1990, p. 330).

Therefore, the general principle is that employers may not conduct such monitoring except in specific cases and under strict conditions. While the employment relationship places employees under the employer's authority and supervision according to the principle of legal dependency, this does not imply a waiver of the employee's right to private life (Bennour, 2016–2017, p. 251).

2.2.2. Technological Monitoring of Employee Communications within the Institution

The relationship between employees and information systems has become an inevitable aspect of professional life, making it necessary to examine the information systems utilized to monitor employees' telephone communications as well as their email correspondence.

2.2.2.1. Telephone Communications

Monitoring telephone communications involves, on one hand, eavesdropping on conversations, and on the other hand, recording them utilizing recording devices. The existence of either method constitutes monitoring (Al-Amine, 2000, p. 70).

Most institutions rely on modern technological tools to safeguard their interests and promote productivity. Among the most prominent of these tools are automatic call counters, or so-called call transfer system. These devices, installed in some institutions, record the phone numbers dialed internally and externally via the telephones assigned to employees, with the purpose of monitoring and calculating the cost of employee calls (Qassem, 2011, p. 47).

However, The danger associated with monitoring telephone communications lies in the fact that it can reveal an employee's most private matters without their knowledge. It does not distinguish between professional and personal calls and may extend to the private information of third parties merely because they communicate with the employee (Aqida, 2008, p. 11).

2.2.2.2. Email Hacking

Email is regarded as one of the modern means for electronic transactions provided by the Internet, facilitating electronic communication through the exchange of instant messages (Younes, 2004, p. 393). Part of jurisprudence defined it as “a method that allows written messages to be exchanged between devices connected to an information network". (Ibrahim, 2002, p. 55)

The use of email in the workplace has created several challenges for employers, which has been utilized to justify monitoring. Therefore, email interception has become one of the most important risks to privacy, potentially violating the confidentiality of communications across multiple fields. Hence, general legal principles necessitate that safeguards be established to protect the confidentiality of correspondence within clearly defined limits and regulations (El-Dahbi, 2017, pp. 146-147).

3. The Extent of Economic Institutions’ Compliance with Privacy Laws Following the Integration of Artificial Intelligence in the Workplace

The implementation stage of the employment contract raises a delicate issue concerning the extent to which economic institutions respect the employee’s right to private life, particularly given the expansion of digital monitoring means in the workplace.

3.1. The Limits of Economic Institutions’ Respect for Privacy Protections during the Employment Contract Phase

The utilization of information technology by institutions has prompted legislation to establish numerous principles to guarantee information security.

3.1.1. Compliance with Privacy Laws during Job Applications

Legal systems aimed to regulate the potential misuse of these technologies by establishing legal rules that define the limits of informational intervention and clarify which actions are permissible to prevent the negative effect of information systems.

3.1.1.1. Principle of Legitimacy

This principle requires that the collection and recording of personal information be grounded in the explicit consent of the job applicant (Robert Duffar, 1999, p. 50), except in certain cases provided by law where consent is not required. For instance, the French company SKF stored in its databases information concerning employees' political orientations and membership in labor unions, obtained from job applications submitted to the company without prior consent from the National Commission on Informatics and Liberties. Such conduct falls within the scope of Article 42 of the French Communications Law, which criminalizes unlawful recording and storage.

3.1.1.2. Principle of Oversight and Supervision

An employer may not process applicants' information automatically without consulting the institutional committee and notifying the National Commission on Informatics and Liberties to obtain authorization for such processing. Employers are also prohibited from retaining information beyond the period specified by the national commission, and the retained information is directly relevant to achieving the stated purpose (Diab S. M., 2010, p. 93).

3.1.1.3. Principle of Reassurance

The principle of reassurance guarantees the job applicant's right to access the data recorded about them and the results of its automated processing, enabling them to verify its accuracy, correct errors, and delete any data stored unlawfully (Khelaf, 2010-2011, p. 60). Technical or operational errors may occur when storing or processing information electronically, potentially leading to adverse conclusions about the applicant's private life, which can negatively impact their reputation and professional future (Aguoune, Criminal Behavior of the Cybercriminal, 2011–2012, p. 104). The right to correct information ensures that the individual can reaffirm their true identity and personal integrity (Kayser, 1995, p. 316).

The Algerian legislator has obliged qualified employment agencies, municipalities, and accredited private bodies to take all necessary measures to safeguard personal information associated with job applicants and to impose penalties on anyone who discloses personal information impacting

applicants' private lives. (Law No. 04-19 concerning the appointment of workers and employment monitoring, 2004)

3.1.2. Technical Protection of Digital Information during the Job Application Process

The continuous increase in the use of advanced technological means by economic institutions has made it necessary to provide mechanisms for safeguarding and securing information through:

3.1.2.1. Information Encryption Technology

Encryption is referred to as "a mechanism that safeguards information such as documents, images, or electronic transactions from unauthorized individuals, preventing access or alteration. (Abdelhamid, 2010)" The French legislator defines encryption in Law No. 90-1170 of December 29, 1990, on the Organization of Remote Communications as including "all procedures that, through secret protocols, seek to convert understandable information into incomprehensible information or signals, or perform the reverse operation, employing equipment and software designed for this purpose.

3.1.2.2. Anonymization Technique

This method safeguards the privacy of job applicants by preventing others from gathering, analyzing, or exploiting information associated with the individual, encompassing information that could identify them, without their consent or explicit approval. Therefore, many consider it an effective tool for protecting privacy.

3.2. The Limits of Employers' Compliance for Privacy Requirements during the Employment Contract Period

The reality of smart work environments has necessitated measures to ensure the information security of employees' personal data in the face of advanced workplace technologies.

3.2.1. Guarantees for Safeguarding Employees' Personal Data in the Face of Artificial Intelligence

These guarantees include the following:

3.2.1.1. Digital Security of Employees' Identifiable Information

The French legislator was a pioneer in granting legal protection for personally identifiable information through the enactment of the Information Technology and Liberties Act, which established specific safeguards for the collection, usage, access, transfer, and automated processing of personal data. Furthermore, the law created the National Commission on Information Technology and Liberties as a supervisory body to ensure protection.

Personally information covered by this protection refers to any data that allows, directly or indirectly, the identification of a natural person, regardless of its form or features, whether digital or textual, and or in the form of a still or moving image (Diab S. M., 2001, p. 191).

3.2.1.2. Digital Security of Employees' Health Information

An employee's health directly impacts his ability to perform tasks assigned under the employment contract. As a result, the employer has a legitimate interest in being informed of employees' health status.

The law has sought to provide legal protection to safeguard employees' health, particularly for sick employees, by establishing a legal framework that preserves privacy while ensuring the implementation of preventive measures. The highest level of protection is maintained through professional confidentiality, as required by the multiple medical practitioners involved in the employee's health (Khelaf, 2010-2011, p. 100).

3.2.2. Guarantees for the Legitimacy of Automated Processing of Employees' Personal Data

Information technology is an important component and a fundamental tool for institutions (Diab S. M., 2001, p. 90). However, reliance on IT carries potential risks to employees' rights and freedoms. Thus, the automated processing of information is subject to legal oversight.

3.2.2.1. Legal Regulations on the Automated Processing of Employees' Digital Information

The legal regulations for the automated processing of employees' digital information include:

- **Notification to the National Commission on Information Technology and Liberties (CNIL):**

Automated processing of information in the workplace has become inevitable. Before its implementation, the user must notify the National Commission on Informatics and Liberties. The notification must include a commitment that the processing will comply with legal requirements. Any processing conducted without prior notification is considered illegal.

With regard to the automated processing of employees' medical information, the French legislator extended protection as early as 1994. It sought to strike a balance between respect for the employee's right to privacy with the needs of medical research. The law mandated confidentiality and security for personally identifiable information, specifying the rights and obligations of employees whose data is medical in nature. Moreover, it required notification of the institutional committee followed by the CNIL to obtain authorization before processing (Law No. 94-548 and Law No. 78-17, 1994- 1978).

French legislation supported the automated processing of workers' personal data with criminal protection, as the Penal Code criminalizes the unauthorized electronic processing of personal data under Article L226-16 thereof.

- **Compliance of Automated Processing with the Law**

One of the most significant legal safeguards issued by French legislation concerning the automated processing of an employee's personal data is the requirement that the notification submitted to the National Commission on Information Technology and Liberties include an undertaking that such processing will comply with the requirements of the law.

These procedures seek to monitor the extent to which the employing institution respects the law when performing automated processing of employees' personal data. They are designed to manage both individual and collective monitoring processes to protect employees' privacy, particularly because such processing may include information employed to make

decisions impacting employees' interests within the institution (Diab S. M., 2001, p. 192).

In Algerian legislation, to safeguard the sanctity of private life, the legislator introduced a new Chapter Seven bis into the penal Code, addressing violations associated with the automated processing of data affecting private life in Articles 394 bis to 394 bis 7. Although this intervention in such a sensitive and serious area came relatively late, it is effective(The Algerian legislator intervened in this matter twice: first in 2004 under Law No. 04/15, dated 10/11/2004, concerning Articles 394 bis 3 to 394 bis 7; and second under Law No. 06/23, dated 20/12/2006, concerning Articles 394 bis, 394 bis 1, and 394 bis 2), criminalizing multiple acts committed via computer with the intent to violate private life.

The Algerian legislator also established liability for legal entities committing the acts specified in this law (These provisions are codified in Articles 394 bis, 394 bis 1, and 394 bis 2 of the Algerian Penal Code). Penalties include a fine equivalent to five times the maximum fine applicable to a natural person as the primary penalty, without prejudice to the possibility of imposing additional supplementary penalties under Article 18 bis.

3.2.2.2. Employees' Rights in Relation to Information Technology and Artificial Intelligence

These rights include the following:

- **The Right to Object**

Employees have the right to object to information concerning them that is subject to automated processing. This is a personal right that must be communicated to the employee in advance. It was included in one of the recommendations of the National Commission on Information Technology and Liberties. French legislation affirmed this protection in Article 38 of the amended January 6, 1978 Informatics Law, which largely retained the wording of Article 23 of the original law prior to its amendment in 2004.

Under French law, any natural person may object, for legitimate reasons, to certain personal data being subject to processing, except in cases where the processing is conducted to fulfill a legal obligation or when the right to object has been explicitly excluded by the procedure authorizing the processing(Article 38 of the aforementioned law in paragraphs one and three, Law 1978, as amended, relating to Informatics).

The right to object includes the employee's right to inquire whether any files exist about them within the institution. Employees also have the right to object to automated processing that produces outcomes detrimental to them, such as denial of promotion or transfer to another position (Lyon-Caen G. , 1991, p. 12).

- **The Right to Access and Request Correction**

The right of access is defined as the person's right to know the content of the data concerning them that is subject to processing (Al-Ahwani, 1987, p. 45). This right lays the foundation for the employee's ability to request corrections when necessary. It enables employees to access all information pertaining to them upon submitting a written request to the institution's administration and to correct some or all of this information, provided that the correction is performed under the supervision of the file management or the authority holding the files.

Regarding, the right to correct information ensures that the individual can reaffirm their true identity and personal integrity when it has been compromised in the eyes of others by incorrect information(Art. 26 of the Law of January 6, 1987, and Article 26 of the Law of January 6, 1987). Employees must be informed of their right to access information and to correct any incomplete, ambiguous, or inaccurate data.

French law grants employees the right to object to the use of personal data concerning them that is subject to processing (Art. 26, Law of January 6, 1987). Article 39 of the amended 1978 Information Technology Law provides that every employee has the right to consult the data controller to verify that personal data regarding them is being processed correctly, or to ensure that such processing is not taking place.

4. CONCLUSION

This study demonstrated that the transition toward smart work environments, despite the opportunities it provides for enhancing performance and efficiency, presents real challenges concerning the safeguarding of digital privacy and the protection of employees' professional rights. The analysis indicated that artificial intelligence and

electronic monitoring in the workplace can shift from being productivity-enhancing tools to instruments that threaten digital privacy if not regulated within a clear and balanced legal framework. The study also emphasized that compliance with international data protection standards remains uneven across institutions, highlighting the need for stronger legal and ethical oversight of smart technologies in work environments.

Firstly : Results

- Digital privacy has become an integral element of professional rights, and any violation directly affects the quality of the work environment.
- The expended use of electronic monitoring tools may breach the principles of proportionality and necessity, undermining trust within institutions.
- International legislation provides an advanced framework for data protection, yet institutional implementation often suffers from gaps in transparency and compliance.
- Integrating artificial intelligence into employee performance evaluations may introduce algorithmic biases that impact professional fairness unless subject to effective oversight.

Secondly: Recommendations

- The necessity of adopting clear national legislation regulating the protection of digital privacy in the workplace and determining the limits of electronic monitoring.
- Requiring institutions to adopt transparent policies for data collection and processing, while ensuring workers' right to access and correct their data.
- Adopting the principle of data minimization to avoid excessive monitoring, limiting data collection to what is strictly required for professional purposes.
- Establishing institutional compliance and oversight mechanisms to monitor the use of artificial intelligence technologies and ensure respect for workers' digital rights.

- Fostering training and awareness within institutions concerning the risks of electronic monitoring and the means of safeguarding personal data.

5. Bibliography List:

Abdelhamid, R. (2010, 12). *Security of Electronic Information Networks: Risks and Solutions.* Consulté le 01 03, 2026, sur Cybrarians Journal, Issue 30: http://www.journal.cybrarians.org/.

Aguoune, H. B. (2011–2012). Criminal Behavior of the Cybercriminal. *Master's Thesis in Criminology and Punishment*. Batna: Faculty of Law and Political Science, University of El Hadj Lakhdar .

Aguoune, H. B. (2011–2012). Criminal Behavior of the Cybercriminal. *Master's Thesis in Criminology and Punishment*. Batna: Faculty of Law and Political Science, University of El Hadj Lakhdar.

Al-Ahwani, H. E.-D. (1987). *The Right to Respect for Private Life (The Right to Privacy).* Egypt: Dar Al-Nahda Al-Arabiya.

Al-Amine, S. (2000). *Telephone, Audio, and Video Surveillance.* Egypt: Dar Al-Kitab Al-Dhahabi,.

Aqida, M. A.-U. (2008). *Monitoring Telephone Conversations: A Comparative Study.* Egypt: Dar Al-Nahda Al-Arabiya.

Bennour, S. (2016–2017). Protection of Employees' Private Life. *Doctoral Dissertation in Legal Sciences, Specialization in Private Law,*. Algeria: Faculty of Law and Political Science, University of Oran 2.

CNIL. (s.d.). *Artificial intelligence is a logical and automated process generally based on an algorithm and capable of performing well-defined tasks.".* Consulté le 12 26, 2025, sur Glossary of Artificial Intelligence (AI).: https://www.cnil.fr/fr/intelligence-artificielle/glossaire-ia.

Committee For The Corporate Governance Of Listed Companies. (1999). *REPORT CODE OF CONDUCT.* MILANO: Borsa Italiana S.p.A.

Diab, S. M. (2001). *The Employee's Obligation of Honesty and Loyalty in Individual Employment Relationships.* Cairo, Egypt: Dar Al-Nahda Al-Arabiya.

Diab, S. M. (2010). *Legal Protection of Private Life and Its Safeguards in Light of Modern Technological Mean.* Egypt: Dar Al-Kutub Al-Qanuniya,.

El-Dahbi, K. (2017). The Right to Privacy in the Face of Electronic Attacks (Comparative Study),. *Al-Ustadh Al-Bahith Journal for Legal and Political Studies,*, 143–156.

Europe, C. o. (1981, January 28). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Strasbourg: European Treaty Series.

European Parliament Resolution. (2017, February 16). *Artificial intelligence refers to the ability of a machine to reproduce human-related behaviors such as reasoning, planning, and creativity.* Consulté le 12 25, 2025, sur containing recommendations to the Commission on civil law rule: https://www.europarl.europa.eu/news/fr/headlines/society/20200827STO85804/intelligence-artificielle-definition-et-utilisation.

Grévy, M. (1990). Video Surveillance in the Workplace: A Normal Method of Employee Control. *Droit Social No. 4*, 328-342.

HAI. (2020, September). *Human-Centered Artificial Intelligence, Christopher Manning, Artificial Intelligence Definitions.* Consulté le 12 12, 2025, sur Stanford University: https://hai.stanford.edu/sites/default/files/2020-09/AI-Definitions-HAI.pdf

Hallevy, G. (2013). *When Robots Kill.* Boston, United States of America: Northeastern University Press.

Hallevyl, G. (2013). *When Robots Kil.* Boston, United States of America: Northeastern University Press.

Ibrahim, K. M. (2002). *Security of Email Correspondence* . Egypt: Dar Al-Jami'iya.

International Labour Conference. (2004, June). Recommendation No. 195 on Human Resources Development: Education,. *Human Resources Development: Education, Training, and Lifelong Learning,*. concerning guidance on career pathways and training support services, 62nd Session,.

Kayser, P. (1995). *The Protection of Privacy by Law: Protection of the Secret of Private Life.* France: 3rd edition ECONOMICA,.

Khelaf, B. (2010-2011). The Development of Protection of Employees' Private Life. *Master's Thesis in State Transformations*. Algeria: Faculty of Law and Political Science , University of Ouargla, .

Law No. 04-19 concerning the appointment of workers and employment monitoring, p. o. (2004, December 25 -26). Article 20 . Official Gazette, No. 83,.

Law No. 18-07. (2018 , June 10). the Protection of Natural Persons with regard to the Processing of Personal Data. Official Gazette.

Law No. 94-548 and Law No. 78-17. (1994- 1978, July-January 2-6). law on concerning the processing of personal data for research purposes in the field of health, law on Information Technology, Files, and Freedoms.

Law No. 94-548 of 1 July 1994, J. N.-1. (s.d.).

Law No. 94-548 of 1 July 1994, J. N.-1. (1978 , January -).

Lefebvre, S. (1998). *New Technologies and the Protection of Privacy in the Workplace in France and/or Quebec.* France: Aix–Marseille University Press.

Lyon-Caen, G. (1991). *Report for the Minister of Labor, Employment, and Vocatio nal Training "Public Freedoms and Employment",*. Paris: Ministry of Labor, Employment, and Vocational Training.

Lyon-Caen, G. (1992). *Public Freedoms and Employment.* France: La Documentation Française.

Miro Miroslavov. (2024, October 3). *What Is A Smart Workplace? Key Solutions And Consideration.* Consulté le 12 27, 2025, sur https://www.officernd.com/blog/smart-workplace/

Paragraph (b) of Recommendation No. 8 concerning guidance on career pathways and training support services, I. L. (s.d.).

Paragraph (b) of Recommendation No. 8 concerning guidance on career pathways and training support services, I. L. (s.d.).

Qassem, M. H. (2011). *Legal Protection of Employees' Private Life in the Face of Certain Aspects of Modern Technology.* Beirut, Lebanon,: Al-Halabi Legal Publications,.

Ritika. (2024, May 21). *Smart Workplace.* Consulté le 12 2, 2025, sur The Next Generation Guide for Companies: https://www.vizitorapp.com/blog/the-next-generation-guide-for-companies/

Robert Duffar, J. J. (1999). *Human Rights and Fundamental Freedoms.* France: Montcherstion.

Saidani Faiza, ,. ". (2022). The Legal Classification of Robots and the Extent of Their Legal Liability. pp. 408–417.

Younes, O. M. (2004). *Crimes Arising from Internet Use: Substantive Provisions and Procedural Aspects.* Egypt: Dar Al-Nahda Al-Arabiya.