

The Digital Transformation of the Work Environment in Mexico: An Approach to Digital Rights

Alejandro Paul García Hernández¹, Juan Emmanuel Delva Benavides², Jorge Antonio Leos Navarro³

^{1,2,3}Centro Universitario de Ciencias Económico Administrativas (CUCEA), Universidad de Guadalajara, México.

(ORCID: 0000-0002-2859-378X)

(ORCID: 0009-0000-1444-5455)

ABSTRACT: Since the SARS-CoV-2 pandemic, the use of digital tools in Mexico has expanded quickly and has transformed the organization of work. As telework and digital monitoring technologies spread, digital rights have moved from being a niche topic to a concrete set of guarantees needed by a broad segment of workers. This paper examines the digital transformation of the work environment in Mexico through the lens of digital labor rights, with a focus on the right to digital disconnection, telework, biometric systems, geolocation, and workplace video surveillance. It highlights regulatory gaps and implementation problems and offers recommendations aimed at strengthening legal certainty, institutional guidance, and the effective protection of workers' privacy and wellbeing in a digitalized labor market.

KEYWORDS: digital rights; telework; right to disconnect; workplace surveillance; biometrics; geolocation.

I. INTRODUCTION

The rapid advance of information and communication technologies has accelerated the digital transformation of economies and societies. In Mexico, this process intensified during the SARS-CoV-2 pandemic, when a large number of activities that traditionally depended on physical presence were relocated to digital environments and remote forms of organization.

This shift was not merely technological. It also altered labor relations by increasing the use of platforms, software, and devices to coordinate tasks, measure performance, and communicate in real time. As a result, questions that once appeared marginal—such as the limits of connectivity after working hours or the legality of digital monitoring—became central to the everyday experience of workers and employers.

Mexico currently faces a crossroads. Digitalization can improve productivity, expand access to employment, and enable more flexible forms of work. At the same time, it can deepen asymmetries of power, intensify working time through permanent connectivity, and normalize intrusive forms of surveillance. In this context, digital labor rights operate as a necessary counterweight to protect privacy, health, and dignity.

This article analyzes how the legal system is responding to these challenges. It focuses on the emergence of digital rights in labor contexts and the way in which regulation, case law, and institutional guidance are being used—or are still missing—to address new risks created by digital tools at work.

The central questions are: What are the main digital rights at stake in contemporary workplaces? What legal standards and safeguards should govern the use of technologies such as biometric systems, geolocation, and video surveillance? And what regulatory and institutional measures are needed in Mexico to ensure effective protection without undermining legitimate organizational needs?

To answer these questions, the paper is structured in four parts. First, it outlines the most relevant digital rights in labor relations and reviews their foundations. Second, it examines four high-impact areas: the right to digital disconnection, biometric identification systems, geolocation in the workplace, and video surveillance. Third, it analyzes the Mexican context, with special attention to telework and the regulatory treatment of workplace monitoring technologies. Finally, it presents conclusions and recommendations. Ultimately, the goal is to contribute to a more balanced regulatory approach—one that recognizes the benefits of digital transformation while ensuring that technological adoption does not erode fundamental rights.

II. DIGITAL RIGHTS AT WORK

Digital rights at work refer to a set of guarantees that protect workers when labor relations are mediated by digital tools. They include, among others, limits to permanent connectivity, the protection of personal data, transparency in digital monitoring, and

The Digital Transformation of the Work Environment in Mexico: An Approach to Digital Rights

safeguards against disproportionate surveillance. These rights are closely linked to classical labor protections, but they must be adapted to the specific risks posed by contemporary technologies.

A. The Right to Digital Disconnection: Foundations and Legal Evolution

The right to digital disconnection has emerged as a response to the blurring of boundaries between working time and personal time, especially in telework and hybrid arrangements. It aims to ensure that workers are not expected to remain available through digital channels outside their working hours, thereby protecting rest, health, and family life.

Although the right is closely associated with recent telework reforms, its normative foundations are broader. It is linked to the right to rest, to limitations on working time, and to occupational health. Several jurisdictions have incorporated it explicitly into labor or data-protection legislation, often requiring employers to adopt internal policies that define availability, communication rules, and mechanisms to prevent retaliation for disconnecting.

France and Belgium were among the first countries to regulate digital disconnection, and Spain later incorporated it into its Organic Law 3/2018 on the Protection of Personal Data and the Guarantee of Digital Rights. In practice, the right is implemented through organizational measures (such as defining “quiet hours,” limiting after-hours emails, and establishing escalation protocols) as well as cultural change to avoid confusing commitment with 24/7 availability.

From a labor-policy perspective, digital disconnection is also a governance tool. It helps prevent the extension of working time through constant connectivity and reduces psychosocial risks such as burnout. Its effective implementation requires clear rules, training, and monitoring mechanisms that involve both management and workers’ representatives.

B. Biometric Systems: Implementation and Legal Challenges

Biometric systems have become increasingly common in workplaces, particularly for access control, attendance, and identity verification. These technologies can increase security and operational efficiency; however, they also introduce significant risks because biometric identifiers are difficult (or impossible) to change if compromised.

The use of biometrics in labor contexts raises at least four practical and legal issues: (1) identifying who will be subject to biometric processing; (2) defining how long biometric data will be stored; (3) determining who can access the data and under what conditions; and (4) establishing safeguards, protocols, and accountability mechanisms to prevent misuse.

First, the scope of the measure must be clearly defined. Employers should determine which positions or areas truly require biometric controls, avoid “blanket” adoption, and document the necessity of the system in light of less intrusive alternatives.

Second, retention periods must be limited. Biometric templates and related logs should not be stored indefinitely; retention must be tied to the purpose of processing and to the duration of the employment relationship, with secure deletion once the purpose ends.

Third, access must be restricted. Only authorized personnel should handle biometric systems and data, under confidentiality obligations, with technical controls such as role-based access, encryption, and audit logs.

Fourth, employers must adopt protocols and security measures, including incident-response plans and procedures for exercising data-subject rights. Without these safeguards, biometric adoption can easily become a mechanism of excessive surveillance.

From a technical perspective, biometric systems are often classified into two broad categories: (a) physiological or physical biometrics, which rely on unique bodily features, and (b) behavioral biometrics, which analyze patterns of behavior. This distinction matters because both categories can enable identification and profiling, but their intrusiveness and risks may differ.

Figure 1. Stages of biometric data processing (own elaboration).

TABLE I. STAGES IN BIOMETRIC DATA PROCESSING (OWN ELABORATION BASED ON INAI, 2018).

Operationally, biometric data processing can be understood as a sequence of stages (Table 1): registration (capturing samples), conversion (transforming the sample into a template), storage, comparison (matching against stored templates), and decision (automated or human-assisted). Each stage introduces vulnerabilities and requires tailored safeguards.

A core legal dilemma is that biometric data may reveal sensitive information beyond mere identification. Depending on the modality, biometric samples can disclose health conditions, ethnic origin, disabilities, or other sensitive attributes, increasing the potential harm in case of unauthorized access or secondary use.

In the European Union, biometric data are generally treated as a “special category” of personal data under the General Data Protection Regulation (GDPR). Processing is, as a rule, prohibited unless a specific legal basis applies—such as explicit consent or another exception provided by law—combined with strict necessity and proportionality requirements.

At the global level, comprehensive regulation of workplace biometrics remains limited. Where standards exist, they typically emphasize risk assessment, purpose limitation, data minimization, strong security controls, and independent oversight as key elements of a lawful and legitimate deployment.

Spain offers an influential example in this regard. The Spanish Data Protection Agency (AEPD), in its guidance on biometric presence-control systems (November 2023), stresses that biometric processing in employment settings is high-risk and must be justified by necessity, not convenience. It also warns about power imbalances that can undermine the validity of consent in labor relations.

The Digital Transformation of the Work Environment in Mexico: An Approach to Digital Rights

As a result, organizations are expected to conduct a Data Protection Impact Assessment (DPIA) before implementing biometric systems in many cases, and to demonstrate that the measure is suitable, necessary, and proportionate (a “triple test”) compared with less intrusive alternatives (such as cards, PINs, or other authentication methods).

In short, biometric systems in the workplace require specific legal and institutional guidance. Clear rules on lawful bases, retention, access controls, transparency, and accountability are essential to prevent these technologies from becoming a permanent infrastructure of surveillance.

C. Geolocation in the Workplace: Legal Implications and Regulatory Challenges

Geolocation technologies (GPS and related tools) are increasingly used by employers to coordinate tasks outside traditional workplaces, optimize routes, and monitor service delivery. While they may be legitimate for operational purposes, they also enable continuous tracking and therefore pose serious privacy risks.

The legality of workplace geolocation depends on whether the measure is justified by the nature of the work and whether it is implemented within strict limits. As with other monitoring tools, geolocation should not be treated as a default option; it requires a case-by-case assessment of necessity and proportionality.

A recurring concern is “function creep”: data collected to optimize logistics can later be used for disciplinary purposes, profiling, or intrusive supervision. Without clear safeguards, geolocation can undermine trust and create a permanent sense of being watched. Therefore, regulatory standards typically require that geolocation be linked to explicit, legitimate purposes (such as safety, fleet management, or delivery verification), and that any secondary use be compatible with those purposes and duly justified.

Guidance from legal practice highlights key limits. For example, geolocation must operate only during working hours, and workers should be able to deactivate tracking outside the workday. Employers should also avoid excessive or permanent monitoring and clearly communicate whether the device is for strictly work purposes or allows private use.

Because location information can identify or single out an individual, geolocation data are personal data and must be processed under data-protection principles, including purpose limitation, data minimization, transparency, and security.

These principles entail, at minimum: (a) prior information to workers and, where applicable, to workers’ representatives; (b) a clear description of the system, its purposes, and the data collected; and (c) documentation showing why the system is necessary for the job performed.

In employment relations, relying on “consent” is often problematic due to the imbalance of power between employer and worker. For that reason, a lawful basis grounded in legitimate organizational needs and compliance with labor and data-protection limits is usually required, accompanied by safeguards to prevent abuse.

Transparency is indispensable. Workers must be informed—before the system is activated—about when tracking occurs, who will access the data, how long the data will be stored, and how they can exercise their rights.

Retention should be limited. Practice-based guidance suggests that location data should be kept only as long as necessary for the stated purpose; in any case, storage should not be extended beyond what is justified by operational needs and legal obligations (for example, some guidance indicates that retention should not exceed two months as a general limit).

Security measures are also crucial: restricted access, encryption, secure storage, logging of access and modifications, and clear procedures for responding to incidents or unauthorized access.

Workers should be able to exercise data-protection rights, including access to their data, rectification of inaccurate information, and, where appropriate, deletion or limitation of processing. Effective remedies are necessary to prevent geolocation from becoming an instrument of arbitrary discipline.

From an enforcement perspective, non-compliance can entail administrative sanctions, labor disputes, and the exclusion of unlawfully obtained evidence. This strengthens the incentive for employers to build compliant systems from the start.

In Mexico, geolocation in employment settings remains under-regulated. The lack of specific standards increases legal uncertainty and makes it harder to balance legitimate business interests with workers’ privacy.

Accordingly, Mexico would benefit from sectoral guidelines or regulatory provisions that clarify lawful bases, transparency requirements, retention limits, and the role of worker participation in decisions to deploy geolocation systems.

D. Workplace Video Surveillance: Legal Implications and Tensions with Fundamental Rights

Video surveillance is widely used in workplaces for security, loss prevention, and, increasingly, for performance monitoring. Cameras can protect people and property, but they also intrude into the private sphere when they capture identifiable individuals and record their behavior in detail.

In European data-protection frameworks, video recordings that identify a person are personal data and must comply with principles such as legality, purpose limitation, data minimization, and transparency. Informational signage, access restrictions, and defined retention periods are typically required, and the use of cameras must be justified and proportionate to the purpose pursued.

In the labor context, video surveillance creates a structural tension between the employer’s managerial power and the worker’s rights to privacy and dignity. Case law has often applied a proportionality analysis, asking whether monitoring is suitable, necessary,

The Digital Transformation of the Work Environment in Mexico: An Approach to Digital Rights

and balanced, and whether workers were informed. Covert surveillance tends to be treated as exceptional and requires strict justification.

Recent guidance at the European level also stresses that surveillance must not become “continuous observation” by default. Employers should choose the least intrusive means and ensure that monitoring does not extend to areas such as restrooms, locker rooms, or rest areas, where expectations of privacy are especially high.

In Mexico, digital-transformation policies have promoted the expansion of connectivity and digital infrastructure. The legal framework supporting these efforts has been articulated around multiple axes, including open data policies and the development of digital identity and interoperability mechanisms.

In addition, digital-skills initiatives seek to reduce the digital divide and foster inclusion so that workers and organizations can adopt technologies more effectively. Connectivity policies, in turn, aim to expand broadband access as a condition for remote work and digital services.

Within this broader context, workplace surveillance technologies—such as video systems—have become more accessible and more common. Yet their adoption has not always been accompanied by clear internal protocols or by adequate privacy governance.

As a result, organizations frequently implement cameras for multiple purposes at once (security, discipline, productivity), which increases the risk of function creep and makes it difficult to ensure that processing remains compatible with the original purpose.

From a regulatory standpoint, this area raises several challenges. These include the need for clear information to workers, limits on who can access recordings, secure storage, retention rules, and safeguards against discriminatory or abusive uses.

In practice, the most relevant challenges include: (a) the absence of specific labor-oriented standards on video surveillance; (b) the use of recordings as evidence in disciplinary processes without clear chain-of-custody and legality safeguards; (c) potential use of advanced analytics (including facial recognition) that increases the intrusiveness of monitoring; (d) weak institutional oversight and low levels of worker awareness; and (e) the normalization of surveillance cultures that erode trust and may chill legitimate workplace participation.

From a rights-based perspective, video surveillance must be assessed under necessity and proportionality. Legitimate purposes such as safety do not automatically justify broad monitoring, and the scope of recording should be limited to what is indispensable.

Moreover, transparent information is a minimum condition: workers should know that they are being recorded, the purpose of the system, and how to exercise their rights. Internal policies should specify who can view recordings and under which circumstances, and should include procedures to prevent unauthorized access.

Retention limits matter as well. General practice in data-protection systems is to keep recordings for short periods (often around one month) unless a specific incident requires preservation for legal proceedings. Indefinite storage is difficult to justify and increases risk.

Video surveillance should also be integrated into broader compliance programs. Risk assessments, training, and periodic audits can help align monitoring practices with legal duties and reduce the likelihood of abuse or data breaches.

In short, workplace video surveillance sits at the intersection of labor law, privacy, and technological governance. Without clear rules and institutional guidance, surveillance can easily exceed legitimate limits and undermine fundamental rights.

For Mexico, a priority is to clarify standards through labor-oriented regulation and administrative guidance that defines lawful purposes, transparency duties, retention rules, and remedies. These standards should be coordinated with data-protection principles and should encourage worker participation.

Strengthening oversight and promoting a culture of privacy at work are essential steps to ensure that video surveillance remains an exceptional and justified tool rather than an all-purpose instrument of control.

III. DIGITAL RIGHTS AT WORK IN MEXICO

The Mexican case illustrates both progress and pending challenges. Telework regulation advanced rapidly after the pandemic, but the governance of workplace monitoring technologies remains fragmented. The following subsections examine telework and the legal treatment of surveillance tools in Mexico.

A. Regulatory Evolution and Practical Reality of Telework in Mexico

Telework is not entirely new in Mexico, but it expanded dramatically during the SARS-CoV-2 pandemic as organizations sought to maintain operations while reducing physical contact. This expansion exposed regulatory gaps and accelerated reform efforts.

On 12 January 2021, reforms to the Federal Labor Law (Ley Federal del Trabajo, LFT) introduced a dedicated framework for telework (home office), defining it as work performed more than 40% of the time outside the employer’s premises using information and communication technologies. The reform sought to provide legal certainty and minimum guarantees for both workers and employers.

Among other obligations, the LFT framework requires employers to provide, install, and maintain the equipment needed for telework, to assume or share costs related to telecommunications and electricity, to respect the right to digital disconnection at the end of the workday, and to implement policies on information security and data protection.

The Digital Transformation of the Work Environment in Mexico: An Approach to Digital Rights

The reform also places emphasis on occupational health and safety. Telework environments can create ergonomic and psychosocial risks, especially when working hours become blurred and when performance pressure is mediated by digital tools.

To operationalize these duties, Mexico adopted the Official Mexican Standard NOM-037-STPS-2023 on safety and health conditions in telework. The standard reinforces preventive approaches by requiring risk identification, ergonomic measures, training, and coordination mechanisms between employer and worker.

Nevertheless, implementation remains uneven. Many organizations adopted telework under emergency conditions without adequate policies, and later struggled to formalize agreements, provide equipment, or define boundaries on availability.

A persistent challenge is cultural: the expectation of permanent connectivity can persist even when formal rules recognize digital disconnection. Without internal enforcement and leadership commitment, the right may remain nominal.

Telework also raises data-protection issues because work is performed on networks and devices that may combine personal and professional use. This increases the exposure of personal data and makes it essential to define security protocols and responsibilities. From a labor-relations standpoint, telework can also affect collective dynamics, supervision practices, and evaluation systems. Digital monitoring tools may be introduced as substitutes for physical supervision, intensifying surveillance and raising privacy concerns.

Empirical evidence suggests that telework adoption is heterogeneous: some sectors and occupations can work remotely with relative ease, while others face connectivity limitations, inadequate home environments, or organizational resistance. This means telework may reproduce or deepen existing inequalities.

Surveys referenced in public discussions indicate that a significant share of employers perceive difficulties in guaranteeing digital disconnection for some positions, particularly where responsibilities are linked to continuous service or international coordination. At the same time, worker awareness of their digital rights remains limited. Even when legal standards exist, many workers do not know the scope of protections or how to claim them, which weakens the practical impact of reform.

These dynamics point to a need for stronger institutional guidance, model policies, and capacity-building. Telework rules must be translated into concrete organizational practices, with monitoring mechanisms and dispute-resolution pathways.

Finally, telework intersects with other technologies discussed in this paper—biometrics, geolocation, and video surveillance—because employers may deploy these tools to monitor remote work. This makes it essential to ensure that telework governance includes privacy safeguards.

In sum, Mexico has made important steps in telework regulation, but effective implementation requires enforcement, training, and a coherent framework that addresses the broader ecosystem of digital monitoring technologies.

B. Workplace Video Surveillance: Legal Framework and Regulatory Challenges

In Mexico, workplace video surveillance is often justified under employers' general managerial powers and the need to ensure security. However, the absence of detailed labor-specific standards means that practices vary widely and are sometimes adopted without adequate transparency.

Legal commentary and practice note that electronic evidence—such as video recordings—can be admissible in labor proceedings if obtained lawfully and without violating morality or fundamental rights. For that reason, it is commonly recommended that employers inform workers in writing about the installation of cameras, specify the purposes of recording, and regulate access to footage through internal policies.

Despite these practical recommendations, Mexico still lacks comprehensive guidance on proportionality, retention, and permissible locations for cameras. Clear administrative standards and internal compliance programs are therefore essential to reduce disputes and protect workers' rights.

C. Processing of Biometric Data: Progress and Challenges in Mexican Regulation

Mexican data-protection law recognizes that biometric data can be sensitive personal data, especially when it enables unique identification. In workplace settings, biometrics are frequently used for attendance and access control, which makes it important to define lawful purposes and strict safeguards.

The National Institute for Transparency, Access to Information and Personal Data Protection (INAI) has issued guidance on biometric data processing, emphasizing transparency, purpose limitation, security measures, and accountability. However, these are general data-protection standards and do not fully resolve labor-specific issues such as consent validity, proportionality, or alternatives.

A more detailed framework—through regulations, sectoral guidelines, or case law development—would help reduce uncertainty and prevent biometric systems from becoming routine tools of intrusive surveillance.

D. Socialization of Digital Rights: Unfinished Business

A key pending issue is the socialization of digital rights—that is, ensuring that both workers and employers understand these rights and how to implement them. Legal recognition is insufficient if rights are not known, internalized, and operationalized in daily practice.

The Digital Transformation of the Work Environment in Mexico: An Approach to Digital Rights

In many organizations, digital rights are treated as compliance requirements rather than as part of labor governance. This leads to minimal policies that exist “on paper” but do not change behaviors, especially regarding after-hours connectivity and monitoring practices.

Moreover, low awareness among workers makes it difficult to exercise rights, request information, or challenge disproportionate measures. This is particularly relevant for groups with less access to legal advice or with greater vulnerability in the labor market. Therefore, training, model policies, and participatory mechanisms—including collective bargaining and worker representation—are crucial to turn digital rights into effective protections rather than symbolic statements.

IV. CONCLUSIONS AND RECOMMENDATIONS

The digital transformation of work in Mexico has accelerated quickly and is likely to continue. This transformation has increased the relevance of digital labor rights, particularly those that protect privacy, rest, and dignity in technologically mediated workplaces. Telework regulation represents a significant step forward. By defining telework, setting minimum employer obligations, and recognizing the right to digital disconnection, Mexico has advanced toward greater legal certainty and stronger protections.

However, important challenges remain. Digital disconnection is difficult to implement without organizational and cultural change, and many workers still lack awareness of the right. Enforcement and guidance are necessary to avoid a gap between formal recognition and actual practice.

In parallel, technologies such as biometrics, geolocation, and video surveillance are being adopted rapidly, often faster than legal standards can adapt. These tools can serve legitimate purposes, but they also create risks of disproportionate surveillance, function creep, and discrimination.

A coherent approach requires integrating labor regulation with data-protection principles. Organizations should be required—or strongly encouraged—to document necessity, minimize data, limit retention, restrict access, and adopt clear internal protocols that enable transparency and accountability.

From an institutional perspective, Mexico would benefit from more detailed administrative guidance on workplace monitoring technologies, including model policies, criteria for proportionality, and best practices for impact assessments and auditing.

Based on the analysis, the following recommendations are proposed:

1. Consolidate the practical implementation of the right to digital disconnection through internal policies, training, and mechanisms that prevent retaliation and ensure compliance across managerial levels.
2. Develop specific guidelines for workplace biometrics that clarify lawful bases, address consent limitations in labor relations, require strong security measures, and promote less intrusive alternatives where feasible.
3. Establish clear standards for workplace geolocation, including strict purpose limitation, transparency duties, deactivation outside working hours, restricted access, and retention limits proportionate to operational needs.
4. Adopt labor-oriented rules for video surveillance that define permissible locations, prohibit monitoring in sensitive areas, regulate access to recordings, and set retention limits, complemented by worker information and participation.
5. Strengthen institutional oversight and coordination between labor authorities and data-protection authorities to address emerging technologies, including AI-based analytics, in a timely and rights-respecting manner.
6. Promote the socialization of digital rights through awareness campaigns, capacity-building, and the inclusion of digital-rights clauses in collective bargaining and workplace governance.

In conclusion, the goal is not to block digital innovation, but to ensure that digitalization advances within a framework that protects fundamental rights. Regulatory clarity, institutional guidance, and organizational responsibility are essential to achieve a balanced and sustainable digital future of work.

REFERENCES

- 1) Ángeles, E., La desconexión digital y su relación con la privacidad de los trabajadores: una revisión de la literatura científica, Perú, Repositorio de la Universidad Privada del Norte, 2021.
- 2) Asociación de Internet MX, "Desconexión laboral, un derecho para los que realizan trabajo remoto", México, 2021, disponible en: <https://www.asociaciondeinternet.mx/estudios/desconexion-laboral-un-derecho-para-los-que-realizan-trabajo-remoto/>
- 3) Comisión Económica para América Latina y el Caribe, A digital path for sustainable development in Latin America and the Caribbean, Santiago, CEPAL, 2022.
- 4) Díaz, S. F. y Maillmann, F., "Pandemia y Teletrabajo", en Solanet, M. A. (ed.), Pandemia: los desafíos múltiples que en el presente le plantea al porvenir, Ciudad Autónoma de Buenos Aires, Academia Nacional de Ciencias Morales y Políticas, 2020, pp. 101-125.
- 5) ECIIA, "México: La conexión digital como garantía del Derecho Humano al Internet y sus implicaciones en materia laboral", México, 2020, disponible en: <https://ecija.com/noticias/mexico-la-conexion-digital-como-garantia-del-derecho-humano-al-internet-y-sus-implicaciones-en-materia-laboral/>

The Digital Transformation of the Work Environment in Mexico: An Approach to Digital Rights

- 6) García, I., Derechos digitales de los trabajadores, España, Universidad de León, 2021.
- 7) Gómez Macfarland, C. A., El teletrabajo, un estudio comparado, México, Instituto Belisario Domínguez, Senado de la República, 2020.
- 8) Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, Guía para el Tratamiento de Datos Biométricos, México, INAI, 2018. Available at: https://inicio.inai.org.mx/documentosdeinterres/guia_datos_biotmetricos_web_links.pdf
- 9) Agencia Española de Protección de Datos (AEPD), "Guía de tratamientos de control de presencia mediante sistemas biométricos", España, noviembre 2023, available at: <https://www.aepd.es/guias/guia-control-presencia-biometrico.pdf>
- 10) Katz, R., Oportunidades para la transformación digital productiva: evidencia estadística sobre el nivel de digitalización sectorial en América Latina y el Caribe, Santiago, Comisión Económica para América Latina y el Caribe (CEPAL), 2024.
- 11) Kurczyn Villalobos, P., "El sello del COVID-19 en los derechos humanos laborales", en Corzo Sosa, E. y González Pérez, L.R. (coords.), Derechos humanos: La década covid en México, México, Universidad Nacional Autónoma de México, 2023, pp. 185-202.
- 12) Lombarte, A. R., "Una nueva generación de derechos digitales", Revista de estudios políticos, España, núm. 187, 2020, pp. 101-135.
- 13) Messenger, J.C., "Introduction: Telework in the 21st century -- an evolutionary perspective", en Messenger, J.C. (ed.), Telework in the 21st Century: An Evolutionary Perspective, Cheltenham, UK y Northampton, MA, USA, Edward Elgar Publishing, 2019, pp. 1-34.
- 14) Moreno, J., "¿Puedo usar un sistema de geolocalización para mis empleados?", España, Lean Abogados, 2021, disponible en: <https://www.leanabogados.com/abogados-laboralistas/sistema-de-geolocalizacion-para-empleados/>
- 15) Poquet, R., El teletrabajo: análisis del nuevo marco jurídico, Pamplona, Aranzadi, 2021.
- 16) Protection Report, "Qué hay que poner en el cartel de videovigilancia RGPD", España, 2022, disponible en: <https://www.protectionreport.com/articulos/rgpd/cartel-videovigilancia-rgpd/>
- 17) Ríos, J., "Videograbaciones de vigilancia, válidas para despedir a trabajador", México, IDC Online, 2021, disponible en: <https://idconline.mx/laboral/2021/12/20/videograbaciones-de-vigilancia-validas-para-despedir-a-trabajador>
- 18) Rodríguez Escanciano, S., Derechos laborales digitales garantías e interrogantes, España, Aranzadi, 2019.
- 19) Secretaría de Trabajo y Previsión Social, "Boletín Número 032/2023", México, STPS, 2023, disponible en: <https://www.gob.mx/stps/prensa/emite-la-stps-disposiciones-obligatorias-para-garantizar-condiciones-de-seguridad-y-salud-en-el-teletrabajo>
- 20) STSJ DE MADRID, Sentencia núm. 763/2019 de 12 de julio, España, Tribunal Superior de Justicia de Madrid, 2019.
- 21) Taléns Visconti, E., "El derecho a la desconexión digital en el ámbito laboral", Revista Vasca de Gestión de Personas y Organizaciones Públicas, España, núm. 17, 2019, pp. 150-161.
- 22) Thales, "How FIDO 2 passkeys can help achieve compliance with GDPR, CCPA and PSD2", Thales (CPL), 2021, available at: <https://cpl.thalesgroup.com/blog/data-security/fido2-authentication>
- 23) Tribunal Superior de Justicia de Castilla y León, Sentencia de 3 febrero 2016, Recurso de Suplicación núm. 2229/2015, España, 2016.
- 24) Vidal, P., "Black mirror ya está aquí (o nuevas formas de control laboral)", Actualidad jurídica Aranzadi, España, núm. 938, 2018.