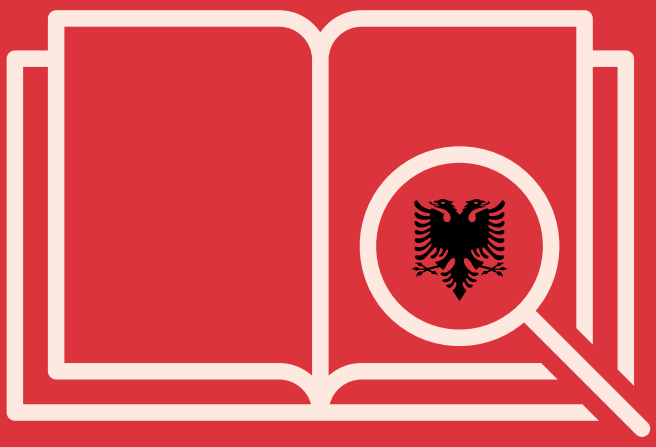
STUDY

Gertjana Hasalla
April 2026

Negotiating Digitalised Workplaces

Rights and Obligations, Albania



Friedrich Ebert Stiftung

Imprint

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

Publishing department
Division for International Cooperation |
Global and European Policy

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

Contact
Blanka Balfer
blanka.balfer@fes.de

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

April 2026

ISBN 978-3-98628-870-9

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

Friedrich Ebert Stiftung

Gertjana Hasalla
April 2026

Negotiating Digitalised Workplaces

Rights and Obligations, Albania

Contents

Foreword

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

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

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

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

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

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

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

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

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

1.
Introduction – Technology at Work Is a Labour Issue

You may already be working with digital technologies without having been asked about them. An app to clock in. Software that scores your calls. Dashboards measuring performance. GPS tracking in vehicles. AI screening job applications. Cameras in new places.

These technologies are often presented as technical tools to improve efficiency or service quality. But for workers, they change how work is organised, monitored, evaluated, and controlled.

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

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

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

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

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

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

How to use this country report

This report is written for workers, shop stewards, and trade unions in Albania, where digital technologies such as CCTV, biometric attendance systems, and algorithmic workforce management are spreading rapidly across both public and private sectors. In many workplaces, digitalisation has outpaced social dialogue, leaving workers insufficiently informed about their rights.

The report helps you understand how Albania's labour law, occupational safety and health framework, and strengthened data–protection legislation apply to digitalised workplaces. It supports workers and unions in holding employers accountable where consultation is weak, enforcement is uneven, or digital tools are introduced as *faits accomplis*.

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

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

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

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

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

What this report can do for you

This report is designed to help you:

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

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

How to use this report in practice

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

Section 2: Examples of digital technologies used in workplaces

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

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

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

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

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

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

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

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

Section 5: Filling the Gaps – Bargaining Topic Suggestions

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

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

When can you use the report?

You can use this report at different moments:

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

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

2.
Examples of Digital Technologies Used in Workplaces

Digitalisation is reshaping workplaces across Albania in both public institutions and private enterprises. Employers increasingly rely on new systems to manage attendance, monitor performance and coordinate tasks, reflecting a rapid shift toward data–driven management. These developments are visible across key sectors such as manufacturing, services, logistics and public administration. In manufacturing, companies use automated attendance and monitoring systems to track production and efficiency. In call centres, delivery platforms and logistics services, algorithmic management tools and mobile applications allocate, supervise and evaluate tasks. Public institutions employ biometric identification, digital archiving and access control technologies to enhance service delivery. While these systems can improve coordination and safety, they also raise concerns about fairness, privacy and proportionality in how data are collected and used.

Most digital tools used in Albanian workplaces process personal or identifiable information, including fingerprints, facial images, video footage, geolocation and digital activity logs. Their introduction requires employers to comply with the Law on Personal Data Protection (Law No. 124/2024), the Labour Code and the Law on Occupational Safety and Health, which together require transparency, proportionality and consultation with employees or their representatives (2024–IDP; 1995–LabourCode; 2010–OSH). In practice, such consultation is still limited, and many workers remain unaware of how these technologies affect their rights. Below are present five main types of digital technologies used currently in Albanian workplaces:.

1. CCTV and Video Surveillance Systems

Employers in manufacturing, retail, transport, and public administration often use closed–circuit television (CCTV) systems for security and safety. In Albania, public authorities have recently rolled out “smart city” CCTV networks in 20 municipalities (e.g., Kamëz, Vlorë, Lezhë, parts of Tirana), which operate 24 hours per day and use high–resolution cameras for surveillance and traffic monitoring. These systems may include motion detection or advanced analytics. Any use of CCTV—especially if it involves continuous recording—must remain proportionate and limited to the declared security objectives. Workers should be informed of camera placement, data retention times, and how recordings are used, since video footage constitutes personal data under national law (2024–IDP; 1995–LabourCode).

2. Electronic Attendance and Biometric Timekeeping Systems

Biometric and electronic timekeeping devices are now common in factories, offices and public institutions. Employees clock in using cards, fingerprints or facial scans linked to their working hours. While these systems improve payroll accuracy, they involve sensitive biometric data that require strict safeguards and a Data Protection Impact Assessment (DPIA). Employers must demonstrate necessity and ensure that data are not used for disciplinary or productivity monitoring (2025–KPMG; 2024–IDP).

3. Workforce Management Software and Mobile Applications

In logistics and platform–based work, mobile applications track routes, record performance and evaluate efficiency through algorithmic scoring. These systems collect location and behavioural data continuously, which can lead to opaque or automated decisions. Employers must clearly inform employees about data collection and guarantee human oversight of automated processes (2024–DataprotectionGuidance; 2025–IndustryReports).

4. Call Centre Monitoring and Desktop Tracking Tools

Employers in customer service and outsourcing sectors use monitoring software to record calls, capture screens and measure productivity through dashboards and analytics. Monitoring may also extend to remote work. Although intended to maintain quality standards, such practices can infringe on privacy if not properly regulated. Employees must be notified in advance about the scope and purpose of monitoring and data must be used only for declared operational reasons (2021–Guardian; 2015–LabourCode).

5. IT Security Logging and Access Control Systems

Banks, public institutions and large enterprises maintain detailed access logs to prevent cyber incidents and ensure compliance with data protection and anti–corruption rules. These systems record user activity, login times and document access. While essential for security, data collection must be limited to legitimate purposes and retention periods must be clearly defined (2025–APDP; 2010–OSH).

Across all sectors, responsible use of digital technologies depends on transparent communication, meaningful worker consultation and respect for privacy and dignity. Adherence to data protection and labour legislation ensures that digitalisation supports safe, fair and human–centred workplaces in Albania (2024–IDP; 1995–LabourCode; 2010–OSH).

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

Albania's legal and institutional framework governing the use of digital technologies at work has evolved in recent years, reflecting both the rapid digitalisation of its economy and the country's gradual alignment with European Union standards. The adoption of the new Law on Personal Data Protection (2024) and strengthened labour and occupational safety provisions provides a coherent foundation for regulating workplace surveillance, algorithmic management and automated decision–making.

However, enforcement remains uneven and many employers are unaware of their consultation obligations. Trade unions can use these laws strategically to strengthen worker protection and social dialogue. Together, they offer tools for ensuring that digitalisation in Albania respects human rights, privacy and decent work principles.

- **Law No. 124/2024 "Law for the protection of personal data" and related guidance from the Information and Data Protection Commissioner;** The Law for the protection of personal data entered into force in February 2025. Several key provisions will take effect in January 2027, including those concerning the obligation to communicate data breaches to affected individuals, the development and approval of codes of conduct, and the rules governing the processing of personal data by public authorities for purposes related to public security, national security, and the prevention or prosecution of criminal offences. The law gives workers and their representatives the right to request access to Data Protection Impact Assessments before monitoring or high–risk digital systems are introduced. Worker consultation rights are further reinforced through Article 35 paragraph nine, which requires the controller to seek the views of data subjects or their representatives during the DPIA process whenever appropriate.
- **The Labour Code of the Republic of Albania dated 12.07.1995 (as amended in 2003, 2008, 2016, 2024);** The Labour Code establishes the right to consultation when technological or organisational changes affect employment conditions.
- **Law No. 10 237/2010 "On Safety and Health at Work" and implementing regulations;** The OSH Law obliges employers to assess psychosocial risks from monitoring or algorithmic management.
- **Law No. 10221, dated 4.2.2010, "On Protection from Discrimination", as amended (hereafter Anti–Discrimination Law);** it transposes core EU equality directives, including Directive 2000/43/EC (Racial Equality) and Directive 2000/78/EC (Employment Equality).
- **Sector–specific and public administration rules on ICT procurement and digital systems;** Public procurement rules ensure accountability for data processing when digital systems are provided by third–party contractors.
- **EU–derived instruments and international influences;** EU and ILO instruments provide standards for human oversight, non–discrimination and ethical use of AI systems.

Below, we set out the key rights you already have when management decides to introduce or use digital technology at work. We do this law by law, pointing you directly to the specific provisions you need to know. Alongside your rights, we also highlight management's legal obligations to you, including duties to consult, ensure system transparency, conduct risk assessments, and more. Then, in the next section, we bring this together into two practical sets of questions you can use to hold management to account. The first set covers questions to ask *before* a new digital technology is introduced. The second set covers your *ongoing rights* once the technology is in use. Every question is grounded in existing laws and/or collective agreements. Where management is reluctant to engage or provide answers, we reference the exact legal provisions you can rely on.

Law No. 124/2024 "On Personal Data Protection"

The law entered into force in February 2025. A number of provisions will not apply until January 2027. These include the obligations to communicate data breaches to affected individuals, the creation and approval of codes of conduct, and the rules that regulate how public authorities process personal data for matters related to public security, national security, or the prevention and prosecution of criminal offences.

Coverage:

This law applies to all entities, public and private, that collect, process or store personal data of individuals in Albania. It brings the national framework in line with the European Union's General Data Protection Regulation (GDPR), ensuring that the use of data–driven technologies respects privacy, fairness and proportionality

- → **Art. 5–7**
  Establish the basic principles of lawful, fair, and transparent processing; data minimisation; and purpose limitation.
- → **Art. 12–15**
  Grant data subjects the right to access, correction, erasure, and restriction of processing.
- → **Art. 22–25**
  Regulate the use of special categories of data, including biometric and health–related information, requiring stricter safeguards.
- → **Art. 30–35**
  Define the obligation to conduct Data Protection Impact Assessments (DPIAs) before introducing high–risk technologies and to consult the Information and Data Protection Commissioner where risks are high.
- → **Art. 35 (9)**
  Gives workers and their representatives the ability to request that their views be considered during the preparation of a DPIA when the processing may affect them. This article also allows representatives to seek access to relevant DPIA information that concerns the impact of the planned processing.
- → **Art. 40–45**
  Define the powers of the Commissioner for Information and Data Protection to supervise compliance, conduct inspections, and impose administrative measures.

Relevance to digitalised workplaces:

- → **Lawful, transparent, and purpose–limited processing (Art. 5–7):**
  Employers must ensure that any processing of employee data—such as CCTV footage, biometric identifiers, or digital attendance records—is lawful, transparent, and limited to the specific, declared purpose.
- → **Information and access rights (Art. 12–15):**
  Employees have the right to be informed about the categories of data collected, purposes of processing, and recipients of data, as well as the right to access, correct, or request deletion of their data.
- → **Automated decision–making and profiling (Art. 25):**
  Automated decision–making, including profiling or algorithmic ranking systems, is permitted only under conditions that safeguard human dignity. Workers retain the right to request **human intervention** and to contest automated outcomes.
- → **Data Protection Impact Assessment (DPIA) and consultation duty (Art. 30–35):**
  Employers introducing digital systems that may significantly affect privacy or data security must conduct a **DPIA** in advance and, where risks remain high, must consult the **Information and Data Protection Commissioner (IDP)**.
- → **Art. 35(9)** (mirroring **GDPR Art. 35(9)**) further states that *"where appropriate, the controller shall seek the views of the data subjects or their representatives on the intended processing"*, except where such consultation would endanger commercial confidentiality or security of processing.

  This creates a clear legal basis for **worker or union consultation** during DPIA preparation and review.
- → **Biometric and special–category data (Art. 22–24):**
  Biometric data such as fingerprints, facial images, or voice patterns are considered *special categories* of data and may only be processed when strictly necessary for legitimate aims, with proportionate safeguards and defined retention periods.

This law gives employees strong procedural tools to challenge unlawful data use and to demand transparency from employers about any technology that collects or analyses personal information. (2024–IDP) (2025–Dataprotection-News)

Union relevance

Trade unions can rely on Articles 30–35 to demand participation in DPIAs and on Article 35 (9) to formally request that worker representatives be consulted before new monitoring or algorithmic systems are introduced. They may also cite Articles 12-15 to obtain disclosure of personal data used in disciplinary or performance evaluations.

Practice insight

Several public institutions have introduced biometric attendance systems in recent years, and such rollouts have sometimes produced concerns among staff about privacy and monitoring. In these situations, worker representatives could have relied on Article 35 of Law No. 124/2024 "On Personal Data Protection" to request prior consultation and disclosure of the Data Protection Impact Assessment (DPIA). In parallel, Articles 46–49 and 200 of the Labour Code of the Republic of Albania provide consultation rights requiring employers to inform and discuss with employees or their representatives before implementing technological or organisational changes that affect working conditions.

The Labour Code of the Republic of Albania 1995 (as amended in 2003, 2008, 2016, 2024)

Coverage:

The Labour Code regulates all employment relationships, both in the public and private sectors. It sets fundamental principles for fair employment practices, worker protection and workplace relations

- → **Art. 32**
  Protects the dignity, health, and moral integrity of employees; prohibits practices that violate personal privacy.
- → **Art. 46-49**
  Regulate changes in working conditions and require prior notice and consultation when new technologies or organisational changes affect employees.
- → **Art. 197-202**
  Establish the rights of trade unions and the obligation of employers to consult and negotiate collective agreements.
- → **Art. 200**
  Provides a legal basis for union consultation on technological changes affecting employment or working conditions.
- → **Art. 203-206**
  Define the framework for dispute resolution, mediation, and collective labour conflicts.

Relevance to digitalised workplaces:

- → **Protection of dignity, privacy, and well-being (Art. 32):** Employers are required to respect and protect the dignity, privacy, and physical and mental integrity of employees. This obligation extends to all forms of workplace monitoring, data collection, and digital performance management.

→ **Consultation on changes to work organisation (Arts. 46–49):**
Any change in work organisation, methods, or technology that affects employees' working conditions must be discussed in advance with workers or their representatives in a timely and transparent manner. These articles guarantee that workers are informed and consulted before digital tools are introduced or procedures are modified.

→ **Use of monitoring data in disciplinary actions (Arts. 32 and 202):**
Data or recordings gathered through monitoring systems may not be used for disciplinary or evaluative purposes unless employees were informed beforehand about the monitoring's existence, scope, and objectives. Employers must demonstrate that the data collection respects the principles of fairness and proportionality.

→ **Social dialogue and technological change (Arts. 197–202, especially Art. 200):**
The Code establishes the legal foundation for collective bargaining and social dialogue. Article 200 in particular gives trade unions the right to request consultation and negotiation on technological change, data use, and other workplace measures affecting employment conditions. This article provides unions with a clear procedural route to participate in digital transformation processes.

Through these provisions, the Labour Code ensures that digitalisation does not erode the fundamental principles of fairness, transparency, and participation in the workplace. (1995–LabourCode)

Union relevance

Under Article 200, unions can require consultation before the implementation of any digital system that changes workloads or performance assessment.

This article provides the legal foundation for participatory governance of workplace technology.

Practice insight

Several public institutions have introduced biometric attendance systems in recent years, which have sometimes raised staff concerns about privacy and surveillance. In such cases, worker representatives could rely on Article 35, paragraph nine of Law No. 124/2024 "On Personal Data Protection" to request participation during the preparation of the Data Protection Impact Assessment and to seek access to relevant information connected to the planned processing and on Articles 46–49 and 200 of the Labour Code to require consultation before system implementation. Used together, these provisions create a strong legal foundation for ensuring that technological changes are transparent, necessary, and jointly reviewed.

Law No. 10 237/2010 "On Occupational Safety and Health" and implementing acts

Coverage:

This legislation applies to all employers and employees and sets comprehensive obligations to identify, assess and mitigate risks related to occupational safety and health (OSH).

- → **Art. 5–8**
  Require employers to identify, assess, and prevent occupational risks in all work processes, including technological change.
- → **Art. 10–13**
  Establish workers' rights to be informed, trained, and consulted on occupational safety and health measures.
- → **Art. 14–16**
  Oblige employers to consult workers or their representatives before adopting new technologies that may impact health or safety.
- → **Art. 19–21**
  Require periodic risk assessments and updates whenever working methods or equipment change.
- → **Art. 22–23**
  Define duties of the Labour Inspectorate to monitor compliance and enforce safety obligations.

Relevance to digitalised workplaces:

- → **Risk assessment of new technologies (Arts. 5, 7–8):**
  Employers must identify and assess all risks arising from the introduction of new technologies, including psychosocial and ergonomic factors linked to continuous digital monitoring, remote work, or algorithmic task allocation. The assessment must be documented and updated whenever new digital tools or working methods are introduced.
- → **Consultation with workers and representatives (Arts. 14–16):**
  Workers and their representatives must be informed and consulted before and during the introduction of new technologies that may affect health or safety. These articles guarantee participatory risk management and require that employees contribute to the design and implementation of preventive measures.
- → **Information and training obligations (Arts. 10–13):**
  Employers must provide adequate information and training on the safe and appropriate use of digital devices, software, and communication systems. Training must include potential ergonomic and psychosocial risks and must be repeated when new equipment or systems are introduced.
- → **Regular review and update of risk assessments (Arts. 19–21):**
  Employers are required to review and update their risk assessments whenever technological or organisational changes occur. Reassessment must include both physical and psychosocial risks and must be shared with worker representatives or OSH committees.

The law encourages proactive risk management and participatory approaches, ensuring that digital tools enhance productivity without compromising workers' health, dignity, or autonomy. (2010–OSH) (2012–ILO)

Union relevance

Articles 14–16 and 19–21 give unions a clear mandate to request participation in risk assessments linked to new technologies or digital monitoring.

Law No. 10221, dated 4.2.2010, "On Protection from Discrimination", as amended (hereafter *Anti–Discrimination Law*).

Coverage:

This law applies to employment, training, and working conditions in both public and private sectors. It protects individuals against discrimination based on gender, race, ethnicity, colour, language, gender identity, sexual orientation, political, religious, or philosophical beliefs, economic status, education, social origin, disability, age, family or marital status, civil status, residence, health, genetic predisposition, or affiliation with a group.

- → **Art. 3–6**
  Define direct and indirect discrimination, harassment, instruction to discriminate, and victimisation.
- → **Art. 7–9**
  Prohibit discrimination in employment, including recruitment, promotion, pay, training, and working conditions.
- → **Art. 33 (1)**
  Establishes reverse burden of proof: once the claimant presents facts suggesting discrimination, the burden shifts to the respondent (employer) to prove that no violation occurred.
- → **Art. 32**
  Provides access to the Commissioner for Protection from Discrimination (CPD), an independent authority empowered to investigate, mediate, and issue binding recommendations or fines.cruitment, promotion, pay, training, and working conditions.

Relevance to digitalised workplaces:

This law is directly useful when algorithmic systems or digital monitoring produce unequal treatment or profiling (for example, biased productivity scoring or unequal promotion outcomes). The reverse burden of proof rule gives workers a procedural advantage, requiring the employer to demonstrate that an algorithm or monitoring tool does not discriminate.

Unions can:

- → File collective or individual complaints with the **CPD.**
- → Use the reverse burden principle in litigation, arbitration, or grievance procedures.
- → Request data disclosure under the **Data Protection Law (Art. 34–35)** to substantiate claims of algorithmic bias.

Sector–specific and public administration rules on ICT procurement and digital systems

Coverage:

Public sector institutions must follow specific procedures when procuring or deploying digital systems, as defined in administrative regulations and the Public Procurement Law. These provisions ensure compliance with data protection, cybersecurity and transparency standards in all public contracts.

Relevance to digitalised workplaces:

- → Contracts with technology providers must explicitly define responsibilities for data processing, retention and access.
- → Public bodies must ensure that any third–party vendor complies with national data protection standards and that all systems include appropriate security measures.
- → Employees whose data are processed through such systems have the right to request information about the purpose, scope and technical functioning of the tools used.
- → Procurement rules promote accountability, ensuring that external service providers cannot process or transfer employee data beyond the agreed contractual framework.

These provisions are particularly important in public administration, where large–scale digital systems handle sensitive personal data of employees and citizens alike. (2025–GovDocs)

Union relevance

Trade unions can use procurement transparency rules to request vendor accountability and prohibit unauthorized employee data transfer.

EU–Derived instruments and international influences

Coverage:

While Albania is not yet a member of the European Union, its legal framework is strongly influenced by EU standards and international labour instruments.

Relevance to digitalised workplaces:

- The principles of the EU General Data Protection Regulation (GDPR) underpin Albania's data protection law, guiding lawful processing, transparency and individual control over personal data.
- The forthcoming EU Artificial Intelligence Act introduces risk–based governance for AI systems, establishing obligations for transparency, human oversight and non–discrimination principles that Albanian policymakers and employers are increasingly adopting.
- International instruments from the International Labour Organization (ILO) and the Council of Europe reinforce these standards, emphasizing the human–centred governance of technological change.

These European and international developments create a dynamic regulatory context that encourages Albanian employers and trade unions to strengthen collective bargaining, risk assessments and ethical safeguards around the use of digital technologies at work. (2016–GDPR) (2023–EUAiDiscourse) (2012–ILO)

Union Relevance

Unions can align bargaining demands with EU standards, reinforcing non–discrimination and transparency obligations for algorithmic tools.

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

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

Usage Note:

The questions below are designed to serve as a practical checklist for trade union representatives, employee councils and occupational health and safety committees. They can be used during negotiations, social dialogue or workplace inspections to ensure that digitalisation is implemented responsibly.

Questions you should ask prior to the introduction of new technologies …

Checklist 1

→ **Has the employer consulted workers or their representatives before deciding to introduce the new technology?**	→ Labour Code Arts. 46–49 and Art. 200; OSH Law No. 10 237/2010 Arts. 14–16	→ Request a consultation meeting and written information on expected changes in work organisation or risks.
→ **What is the specific purpose of the digital technology and how does it support the organisation's operational goals?**	→ Law No. 124/2024 On Personal Data Protection, Arts. 5–7	→ Ask management to clarify goals and operational rationale.
→ **Has management evaluated alternative solutions that would achieve the same purpose with less collection of personal data?**	→ Law No. 124/2024, Arts. 6–7	→ Request documentation of alternatives and data minimization analysis.
→ **Will the technology process personal, biometric, or location data and if so, why is this necessary?**	→ Law No. 124/2024, Arts. 22–24	→ Verify justification and necessity of sensitive data collection.
→ **Has a Data Protection Impact Assessment (DPIA) been conducted and were workers or their representatives consulted?**	→ Law No. 124/2024 Arts. 30–35, especially Art. 35 paragraph nine	→ Confirm participation or request inclusion in the DPIA process.
→ **What types of data will be collected, who will have access and how long will data be retained?**	→ Law No. 124/2024, Arts. 12–15 and 40–45	→ Seek detailed information on data types, access rights, and retention.
→ **Will any automated or algorithmic decisions be made that affect shifts, pay, or performance evaluations?**	→ Law No. 124/2024, Art. 25	→ Request clarity on algorithmic impact and decision-making processes.
→ **How will human oversight be ensured in cases where automated decisions influence employment conditions?**	→ Law No. 124/2024, Art. 25(3)	→ Confirm mechanisms for review and appeal of automated decisions.
→ **Will the system involve a third-party provider and does the contract include data protection clauses?**	→ Law No. 124/2024, Arts. 27–29; Government Procurement Rules (2025–GovDocs)	→ Review contracts or request evidence of confidentiality measures.
→ **Has the employer carried out a health and safety risk assessment on psychological and physical impacts?**	→ Law No. 10 237/2010 On Occupational Safety and Health, Arts. 5, 7, 8, 14–16	→ Ensure the assessment includes psychosocial and ergonomic risks.
→ **What training and information will be provided to workers before the system becomes operational?**	→ Law No. 10 237/2010, Arts. 10–13; ILO Convention No. 155 (2012–ILO)	→ Request schedules and content of training sessions.

Checklist 2

Questions you periodically should ask after the deployment of digital technologies …

→ **Is the system still being used for its original purpose, or has its function changed?**	→ Law No. 124/2024, Arts. 5–7	→ Monitor actual usage and report any deviations from original purpose.
→ **Has management reviewed or updated the DPIA to reflect changes in system functionality or data use?**	→ Law No. 124/2024, Arts. 30–35	→ Request updated DPIA and involvement in review.
→ **Have there been any reported data breaches or security incidents, and were workers informed?**	→ Law No. 124/2024, Arts. 40–45	→ Verify reporting procedures and transparency of incident communication.
→ **Are employees still informed about who has access to their personal data and under what conditions?**	→ Law No. 124/2024, Arts. 12–15	→ Ensure ongoing access awareness and regular updates.
→ **Does monitoring or data collection continue outside working hours, and is this justified?**	→ Law No. 124/2024, Arts. 5–7; Industry Practice Report (2025–KPMG)	→ Evaluate proportionality and legality of off-hours monitoring.
→ **Are procedures in place for workers to challenge or appeal automated decisions affecting employment?**	→ Law No. 124/2024, Art. 25(3)	→ Confirm existence and accessibility of appeal mechanisms.
→ **Have health and safety reviews identified new risks related to stress, surveillance, or workload and what measures were taken?**	→ Law No. 10 237/2010, Arts. 19–21	→ Verify risk mitigation steps and follow-up actions.
→ **Do algorithmic or monitoring systems produce unequal treatment between workers (e.g., gender, age, or status groups)?**	→ 2010–Antidiscrimination Art. 7–9 and 33(1)	→ If disparities appear, request disclosure of system logic and file a complaint to the Commissioner for Protection from Discrimination or initiate collective bargaining on corrective measures.
→ **Has the employer provided proof that automated decisions do not result in discriminatory outcomes, as required under the reverse burden of proof principle?**	→ 2010–Antidiscrimination Art. 33(1)	→ Invoke the reverse burden clause to require documentation showing that the system is neutral and compliant.
→ **Does management conduct regular joint reviews with worker representatives to evaluate digital tools' impact?**	→ Labour Code (1995), Arts. 46–49 and 200	→ Participate in review meetings and document outcomes.
→ **Are all collected data securely stored, and are retention periods respected according to declared purposes?**	→ Law No. 124/2024, Arts. 12–15 and 40–45	→ Inspect storage protocols and retention compliance.
→ **Has the organisation provided updates or refresher training to ensure understanding of technology and data protection?**	→ Law No. 10 237/2010, Arts. 10–13; ILO Convention No. 155 (2012–ILO)	→ Confirm ongoing training and awareness programs.

5.
Filling the Gaps – Bargaining Topic Suggestions

Below are concrete bargaining topics that Albanian workers and their representatives may propose in collective bargaining, workplace agreements or consultation protocols when digital technologies are present. They map directly onto existing law. The items reflect obligations and rights in the Data Protection Law, the Labour Code, and OSH rules, so they are defensible in negotiations and in complaints to regulators (2024–IDP; 1995–LabourCode; 2010–OSH). They respond to real risks observed in Albanian workplaces, such as biometric attendance, GPS tracking in delivery work, desktop monitoring in outsourcing and vendor–controlled algorithms. They give unions concrete leverage. Rather than abstract demands, they create measurable employer duties that can be documented, audited and enforced.

→ Written Purpose and Scope Clause for Monitoring Systems	→ **Employers must provide a written statement at least 14 days before installation of any monitoring or digital management system. The statement must define the system's purpose, scope, data types collected, retention period and legal basis. Any change in purpose requires prior written notice and consultation with worker representatives. (2024–IDP)**
→ Joint Data Protection Impact Assessment (DPIA) and Consultation on Mitigations	→ **Before procuring or introducing high–risk technologies such as biometric or algorithmic systems, employers must conduct a DPIA jointly with worker representatives. The DPIA must include risk identification, agreed mitigation measures and be shared in full at least seven days before deployment. (2024–IDP; 2010–OSH)**
→ Limits on Location Tracking and Off–Hours Data Collection	→ **For roles involving mobile or sensor–based apps, tracking must be limited strictly to working hours. Technical safeguards must prevent data collection outside those periods, except in emergencies or with explicit, time–bound consent. (2024–IDP)**
→ Access and Data Portability Rights in Workplace Disputes	→ **Workers and their authorised representatives have the right to obtain any personal or performance–related data used in disciplinary or evaluation processes. Employers must provide access within five working days of a written request. (1995–LabourCode; 2024–IDP)**
→ Human Review and Appeal Procedure for Automated Decisions	→ **No sanction, pay adjustment, or evaluation outcome may rely solely on automated decision–making. Employees must have the right to request a human review, and employers must provide written reasoning within ten working days. (2024–IDP)**
→ Transparency and Accountability of Third-Party Vendors	→ **Contracts with vendors or software providers must include clauses defining data–processing responsibilities, retention limits, and security standards. Vendors must disclose algorithmic functions, audit logs, and agree to independent audits when requested. Export or resale of employee data is prohibited without explicit consent and safeguards. (2025–GovDocs; 2024–IDP)**
→ Limits on Biometric Processing for Routine Tasks	→ **Biometric identifiers such as fingerprints or facial scans may only be used where strictly necessary for safety or access control. Less intrusive alternatives must be preferred. Data retention must be time–limited and biometric data must be securely destroyed after purpose completion. (2025–KPMG; 2024–IDP)**

→ Joint Occupational Health Reviews for Psychosocial Impacts	→ **Employers and worker representatives must jointly review psychosocial risks arising from continuous monitoring, remote work, or algorithmic management at least once per year. The review must include measurable follow–up actions to reduce stress, burnout and digital fatigue. (2010–OSH; 2012–ILO)**
→ Audit Rights and Periodic Joint Reviews	→ **Unions or employee councils have the right to request independent audits of digital systems every twelve months, funded by the employer or through a jointly agreed mechanism. Quarterly meetings should be held to review audit results, system impacts and compliance with data–protection obligations. (2024–IDP)**
→ Training and Upskilling Guarantees When Systems Change Job Content	→ **When new technologies alter job roles or skill requirements, employers must provide paid training or redeployment opportunities before implementation. Training plans must be discussed with worker representatives during procurement or system design. (1995–LabourCode; 2025–GovDocs)**

These bargaining topics are drafted to go beyond minimal legal compliance, and to provide enforceable workplace protections that address common risks from digital systems. Albanian collective agreements rarely cover these topics. Including them would modernise bargaining practice and align labour relations with European digital standards.

6.
Summary Reflections

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

State of play in Albania

Albania has recently updated its data protection framework to align more closely with EU standards, strengthening individual rights and increasing the obligations of data controllers in both public and private sectors. The Labour Code and OSH rules provide general protections but rarely address modern algorithmic management in explicit terms. This results in a legal environment where data protection law strongly constrains processing of personal data, while labour law and OSH provisions provide complementary but sometimes underused protections for dignity and psychosocial risk.

Main gaps and challenges for workers and unions

- → Limited practice of worker consultation on technological procurements, especially in smaller private employers. This gap creates a risk that rights established in the Labour Code and embedded in data protection and OSH rules are not operationalised in workplaces.
- → Enforcement resources and awareness remain uneven, making it difficult for workers to exercise DPIA related rights, to access raw data used in decisions, or to secure joint risk assessments.
- → The platform economy and algorithmic task allocation create transparency gaps when vendors control operational details and data storage. Collective bargaining and contractual clauses can address these gaps.

Paths forward and practical recommendations

- → Unions and federations can organise workshops on data protection and digitalisation to build the capacities of their members.
- → Unions should use data protection obligations to demand DPIA access and vendor transparency.
- → Psychosocial and mental health effects from digital monitoring should be recognised as occupational hazards.
- → Establish a tripartite mechanism with government, unions and employers to monitor digital transformation.
- → Use the Anti–Discrimination Law's reverse burden of proof as a procedural safeguard when algorithmic or data–driven systems produce unequal impacts. The Commissioner for Protection from Discrimination can become a key ally in ensuring fairness in digital workplaces.

Conclusion

Albania's legal framework already provides the tools to protect workers. The next step is for trade unions to use these tools proactively through consultation, collective bargaining and training. By doing so, unions will ensure that technology supports decent work rather than undermines it.

7.
Annex – Links to the Laws Covered

→ **Law No. 124/2024 – "Law for the protection of personal data"**
Official text on the Albanian legal archive (ELI / QBZ): https://qbz.gov.al/eli/ligj/2024/12/19/124/921d3810-ab2a-4e45-bdca-bef3a84b2721 (Legislation info page for *Ligj nr. 124/2024, Për mbrojtjen e të dhënave personale*)

→ **Labour Code of the Republic of Albania (1995) — as amended**
– Official reference listing (QBZ / Official Publishing Center): https://qbz.gov.al/preview/c1c18a6c-5f3e-457d-b931-de505b3c7ed0 (Preview of *Kodi i Punës*)
– Unofficial consolidated reference (WIPO Lex) — includes the 1995 base text and amendments up to 2015 at least: https://www.wipo.int/wipolex/en/legislation/details/20982 (WIPO Lex database entry for *Labour Code, Republic of Albania*)

Note: Albania's **Labour Code has been amended multiple times** (e.g., 2003, 2008, 2016, and likely 2024 changes). The official central database (QBZ) should reflect consolidated updates; for older consolidated texts, WIPO Lex provides archived legal texts.

→ **Law No. 10 237/2010 – "On Occupational Safety and Health"**
– The official PDF as published in the Albanian Official Gazette (Fletorja Zyrtare, https://qbz.gov.al/share/pMIl4WphTpiu0C3IoWQkvg (Official Publishing Center)
– State Labour Inspectorate legislation index (lists Law No. 10 237/2010): https://www.ilo.org/sites/default/files/wcmsp5/groups/public/@ed_protect/@protrav/@safework/documents/policy/wcms_187886.pdf (Inspektoriati Shtetëror i Punës legislative list including *Ligji Nr. 10.237, dt. 18.02.2010, Për Sigurinë dhe Shëndetin në Punë*)

This page is published by the official State Labour Inspectorate, which administers implementation of workplace safety law, and links to the law and sub-legal acts (regulations approved by the Council of Ministers).

→ **Law No. 10 221/2010 – "On Protection from Discrimination"**
Unofficial English PDF (original Albanian anti-discrimination law text): https://rm.coe.int/lmd-updated-version-english-translation/1680a0c1fc (Council of Europe PDF of *Law No. 10 221, dated 4.2.2010*)

This PDF includes an English translation. For the **Albanian original**, official publication is available via the Official Gazette and QBZ; you can search by law number and date there: https://qbz.gov.al/

→ **EU General Data Protection Regulation (GDPR)**
Official EU legislative text (EUR-Lex): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX-%3A32016R0679 (Regulation (EU) 2016/679 – GDPR)

8.
Glossary List

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

A

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

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

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

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

B

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

C

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

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

D

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

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

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

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

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

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

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

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

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

E

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

F

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

H

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

I

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

O

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

P

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

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

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

R

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

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

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

S

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

W

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

About the author

Gertjana Hasalla, MSc., Albanian Center for Population and Development, ACPD, Centre for Labour Rights, CLR

Negotiating Digitalised Workplaces – Rights and Obligations

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

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

Friedrich Ebert Stiftung