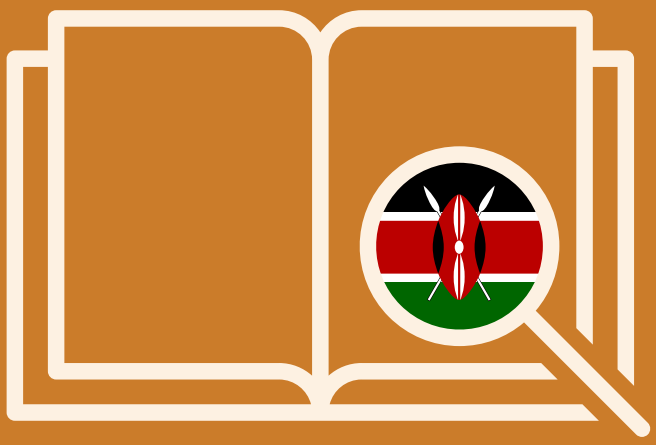
STUDY

Jacqueline Wambui Wamai
June 2026

Negotiating Digitalised Workplaces

Rights and Obligations, Kenya



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
Ludger Stallmeister

June 2026

ISBN 978-3-98628-894-5

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

Friedrich Ebert Stiftung

Jacqueline Wambui Wamai
June 2026

Negotiating Digitalised Workplaces

Rights and Obligations, Kenya

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 Kenyan workers, unions, and negotiators dealing with rapid digitalisation in public services, logistics, call centres, and platform-based work. In Kenya, digital technologies are often introduced alongside outsourcing, platform labour, and non-standard employment, creating sharp power imbalances between workers and employers.

The report shows how constitutional labour rights, data-protection obligations, and occupational safety duties apply to digitally managed workplaces. It helps workers and unions challenge opaque algorithmic management, excessive surveillance, and automated decision-making that affect workers' pay, schedules, and job security.

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 Kenya. 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 provides an overview of 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 Kenya

The eCitizen Government Portal and Integrated Government Digital Systems

Kenya's eCitizen portal has transformed public-service delivery by consolidating more than 22,000 government services into a single digital access point, shifting the public sector from manual, paper-based administration to an integrated, technology-driven system. This transition has fundamentally reshaped the roles of civil servants, moving them from clerical processors of physical documents to digital facilitators responsible for managing online applications, monitoring dashboards, verifying data, and supporting citizens virtually. The shift demands new skills—digital literacy, systems operation, and data management—while introducing data-driven performance oversight that tracks processing times, backlogs, and resolution rates. As government work becomes increasingly digitised, sustained capacity building, structured change management, and strong institutional dialogue are essential to ensure that workers are adequately equipped and supported.

At the same time, this platform raises important workers' rights considerations. Continuous data capture heightens surveillance risks and exposes employees to new forms of accountability pressure if system analytics are misinterpreted or used punitively. Public servants also occupy a dual position under the Data Protection Act (2019): they are both processors of citizens' data and data subjects whose own personal information is recorded within digital government systems. This duality underscores the need for transparent data-governance policies, clear safeguards, and continued negotiation and engagement with unions to protect privacy, ensure fair use of performance data, and maintain worker autonomy in an increasingly digitised public-service environment.[1]

Electronic Keycards/Biometric Access Control Time and Attendance Systems

Biometric and keycard-based attendance systems are now integral to workforce management and security infrastructure across Kenya. Institutions ranging from government ministries and manufacturing firms to banks, schools, and corporate offices increasingly rely on these tools to eliminate manual timekeeping errors, curb proxy clock-in or proxy signings, and ensure accurate payroll processing. The systems are supplied by a mix of local integrators, such as HR Genie, Skillmind Software Limited, Wage Master, and Sanctity Technology Ltd, and distributors of global brands including ZKTeco, AlmiRia, and Tech-Axis. Typically, local companies customize and maintain software while hardware is imported from international manufacturers. The technologies collect fingerprints, facial images, iris scans, and electronic card credentials, storing extracted templates either on-premises or on cloud platforms such as AWS. Integration with payroll systems enables automated wage calculation and compliance monitoring.

Beyond basic attendance tracking, modern platforms provide digital dashboards, analytics, and mobile applications that visualize trends in lateness, absenteeism, overtime, and workforce distribution. These tools support data-driven decision-making, allowing managers to address operational inefficiencies more precisely.

The increasing use of biometric and movement-tracking systems has important implications for labour rights. Workers face heightened surveillance as their physical presence, movement patterns, and biometric identifiers are continuously monitored. Technological errors, such as unreadable fingerprints, faulty facial recognition, or systems that disadvantage workers with disabilities, risk unfair penalties if alternative verification methods are unavailable. Biometric data, once captured, carries long-term risks of unauthorized access, leaks, or misuse, especially where governance frameworks are weak or non-existent. Without transparent communication, informed consent, and regular and active consultation with unions or worker representatives, these systems may undermine trust, erode privacy, and contribute to perceptions of coercive monitoring in the workplace.

1 Gitau, Joseph Gitau (2014), Service Oriented Architecture Model for Integration of E-Government Systems in Kenya: A Case Study of the eCitizen Portal in Kenya (University of Nairobi). Accessed at https://erepository.uonbi.ac.ke/bitstream/handle/11295/99774/Gitau_Service%20Oriented%20Architecture%20Model%20for%20Integration%20of%20E-government%20Systems%20in%20Kenya.a%20Case%20Study%20of%20the%20Ecitizen%20Portal%20in%20Kenya.pdf?isAllowed=y&sequence=1&utm.

Digital Labour Platforms

Kenya's digital labour market is shaped by two major domains: app-based work (ride-hailing, delivery, logistics, on-demand services etc) and global digital outsourcing (data annotation, content moderation, etc). Platforms such as Uber, Bolt, Glovo, Little Cab, and Jumia Food rely on algorithmic systems that automate task allocation, route optimization, pricing, performance evaluation, and wage calculation. Simultaneously, outsourcing firms employ thousands of young Kenyans in data-labelling and content moderation tasks essential to training global AI systems.

These platforms operate through a complex data infrastructure that continuously tracks workers' locations, acceptance rates, delivery times, ratings, and behavioural patterns, systematically exposing them to data privacy and protection violations. While platform work has expanded economic opportunities, particularly for youth, it is characterised by profound informational asymmetries that mask discriminatory biases on pay, task allocations, etc. Workers rarely have insight into how algorithms make decisions and the data they generate remains inaccessible for contestation or correction. This opacity entrenches power imbalances and exposes workers to unpredictable and opaque forms of 'digital discipline' while stifling their constitutional rights to freedom of association and collective bargaining.

CCTV, Biometric and Field-Worker Monitoring Systems

Digital monitoring systems, including CCTV networks, biometric attendance tools, GPS-based vehicle trackers, and mobile monitoring applications, are now standard components of organisational management in Kenya. CCTV cameras monitor premises for security; biometric terminals verify attendance; GPS-enabled applications track field personnel, vehicle routes, fuel consumption, and delivery compliance. Combined, these systems create integrated managerial dashboards that offer real-time visibility over workforce movements and performance metrics.

Much of this infrastructure is supplied by international firms such as ZKTeco, Dahua, and IDEMIA, reflecting Kenya's dependence on imported surveillance technologies. These systems provide efficiency and security benefits, but their widespread deployment raises substantial concerns about privacy, proportionality, and data protection. Location tracking and behavioural analytics can intrusively monitor workers' day-to-day activities, contributing to a climate of continuous surveillance. Without adequate regulation, worker consultation, and clear internal protocols, such monitoring risks being misused for disciplinary action, discrimination, violation of freedom of association rights of workers or intrusive oversight that undermines dignity at work.

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

In Kenya, the relevant Legislation includes:

- → The Constitution of Kenya, 2010
- → Data Protection Act (DPA), 2019, with its accompanying regulations; Data Protection (General) Regulations, 2021; Registration of Data Controllers and Data Processors Regulations, 2021
- → Occupational Safety and Health Act (OSHA), 2007
- → Technical and Vocational Education and Training (TVET) Act, 2013, and The Kenya National Qualifications Framework Regulations, 2018
- → Access to Information Act, 2016
- → The Employment Act, 2007

Relevant Laws and agreements in short

a) The Constitution of Kenya, 2010

This is the supreme law of Kenya, which places sovereign power in the people and establishes a system with strong checks and balances. The key principles and features include the supremacy of the people and the Constitution, the devolution of power, an expansive Bill of Rights (including civil and political rights, socio-economic rights, equality, non-discrimination, and human dignity), separation of powers, and checks and balances among the three branches of government. It also emphasizes leadership and integrity and establishes independent commissions and offices.

b) Data Protection Act, 2019, with its accompanying regulations; Data Protection (General) Regulations, 2021; Registration of Data Controllers and Data Processors Regulations, 2021

This Act governs the protection of personal data and establishes the office of the Data Commissioner. It mandates that personal data, including that of workers[2], must be processed lawfully, fairly, and transparently, and grants individual's rights over their data. The Data Protection (General) Regulations, on the other hand, operationalise Kenya's Data Protection Act by detailing how personal data should be collected, processed, stored, shared, secured, and safeguarded, setting rules on consent, privacy notices, data minimisation, breach notification, children's data, cross-border transfers, and rights of data subjects. The Registration of Data Controllers and Data Processors Regulations, 2021, establish mandatory criteria, procedures, and thresholds for entities that must register with the Office of the Data Protection Commissioner, ensuring accountability and oversight for anyone who determines the purpose of processing personal data in Kenya.

c) Occupational Safety and Health Act (OSHA), 2007

This law is designed to secure the safety, health, and welfare of all individuals in the workplace, including employees and visitors. It sets out general duties for employers and employees, establishes rules for workplace safety committees, and is administered by the Directorate of Occupational Safety and Health Services. The Act also covers aspects such as preventing work-related injuries and illnesses and ensuring that risks to safety and health are managed.

d) Technical and Vocational Education and Training (TVET) Act, 2013, and The Kenya National Qualifications Framework Regulations, 2018

This legislation establishes a framework for regulating the quality and relevance of technical and vocational training. It is essential to ensure that training programmes align with emerging digital skills and job requirements. The Kenya National Qualifications Framework Regulations set the standards, procedures, and quality assurance mech-

2 Note that the Data Protection Act uses the term Data subject, which in this case it has been analysed to include workers.

anisms for developing, accrediting, assessing, and recognising all national qualifications to ensure consistency, comparability, and mobility of learners and workers across education, training, and the labour market.

e) Access to Information Act, 2016

This Act gives effect to the constitutional right of access to information held by the State or any other entity. It can serve as a mechanism for workers or their representatives to request information about the operations and data used by automated or digital workplace systems.

f) The Employment Act, 2007

This Act regulates the relationship between employers and employees, covering contracts, termination, and various employee rights. Section 5 specifically prohibits discrimination and harassment and require **Collective Bargaining Agreements** s employers to promote equal opportunity in employment.

g) Collective Bargaining Agreements

At the time of writing this report, a review of existing collective bargaining agreements (CBAs) revealed that none contained specific clauses addressing digitised workplaces. However, the analysis also noted an important emerging practice: One union had already begun developing draft proposals for the next round of collective bargaining that explicitly seek to address digitised workplace issues, signalling early but significant movement within the labour movement to anticipate and respond to technological changes in workplaces. While still at its early stages, this provides a potential entry point for mainstreaming digital labour protections in future CBAs.

Key Contents of Relevant Laws

a) The Constitution of Kenya, 2010

The Constitution of Kenya lays the foundation for rights in privacy, digitalisation, data protection, access to information, non-discrimination, and labour-related laws, among others.

Coverage: This applies to all persons, and in some parts to citizens and workers across the public and private sectors.

Relevance to digitalisation of work: The Kenyan Constitution guarantees everyone's right to privacy regarding their personal information and private matters, as well as the privacy of communication. This limits how far employers or business owners can go in collecting and tracking personal data. The Constitution anchors the labour rights dimension of Kenya's digital transformation. It ensures that, even in the wake of digitalisation, fair labour practices are upheld and accessible to all workers, regardless of their employment classification, for example, in employment relationships mediated by apps, whether non-standard, remote, or gig.

Why it matters to workers and their organisations: The Constitution gives trade unions and workers, regardless of employment status, a constitutional basis to challenge excessive surveillance, misuse of personal data, unfair labour practices, and even algorithmic control in the world of work. This basis is essential, as it covers all aspects of a worker in every space where they may be deemed to be working, and how far surveillance, or even violations may occur, whether in private or public spaces.

Article 41 is the constitutional guarantee that **fair labour practices** remain valid and enforceable even in the face of automation, remote work, algorithmic control, etc. It is the legal basis for decent work in digitised workplaces. These rights can be claimed in court or even form the basis for legal reforms initiated by workers and their organisations.

Specifically, it provides for the right to fair labour practices for all persons and further guarantees every worker[3] the right to:

- → Fair remuneration.
- → Reasonable working conditions.
- → The right to join, form and participate in trade unions.
- → The right to engage in collective bargaining.
- → The right for trade unions to organise and engage in their own activities, programmes and administration.
- → The right to strike.

Examples in the digital context:

- → Workers in digitised workplaces have, in accordance with article 41 of the Constitution, a right to organise in trade unions and even to collectively bargain, despite their contractual classification.
- → Workers monitored by digital productivity tools or algorithmic management systems may invoke this right if the introduction of technology violates any of the rights as stated above, such as right to fair remuneration.

3 The term worker in this analysis is important as the Constitution uses the term worker which is broader in meaning than that of an employee which is adopted in the Labour Laws. However, it is important to note that no law has defined who a worker is in Kenya.

Article 35 guarantees citizens the right to Information

It provides that every citizen has the right to information, either held by the state or any other person, including a private entity, when necessary for the exercise or protection of any other right or freedom.

The right to information, once invoked, can ensure that workers managed through digital systems can request and access data about themselves, how management decisions are made using digital tools, and any information they need in a digitised workplace.

Examples in the workplace:

- A worker monitored through a digital attendance system or even a productivity system can request to see the data collected about them and how it is used in evaluations, if this information is required to protect the right to non-discrimination or even unfair labour practices.
- Workers can request either performance or audit data from systems like eCitizen to verify how records affect their job performance or pay, if this information could also be used during the exercise of collective bargaining as a fundamental right under *Article 41*.

It is important to note that access to information for private entities, such as business owners, is required for the exercise or protection of fundamental freedoms, such as fair labour practices, the right to strike, fair remuneration, reasonable working conditions, and collective bargaining.

Article 27 serves as the foundational guarantee of **equality and freedom from discrimination** for every person in Kenya.

This article prohibits direct and indirect discrimination against any person on various grounds, including race, sex, pregnancy, marital status, health status, ethnic or social origin, colour, age, disability, religion, conscience, belief, culture, dress, language, or birth.

Discrimination can either be direct or indirect. Direct would mean a clear act of bias, for example, a job stating that "men only" can apply. Indirect discrimination could also mean a seemingly neutral rule or practice that, for example, disproportionately disadvantages a group with a protected characteristic, for instance, ethnicity. This is enforced by the reverse burden of proof, which will be discussed further under the Employment Act.

Article 31 is the bedrock for the right to Privacy in Kenya. It guarantees the right to privacy, including the right not to have the information relating to their family or private affairs unnecessarily required or revealed, and the privacy of their communications infringed.

This is particularly important in the digitised world of work, where platforms can collect massive amounts of data and where monitoring and surveillance are the norm, which may infringe on the right to privacy.

Table 1

Table 1: Main articles in the Constitution of Kenya, 2010

Article	Content / Right	Relevance to Digitalised Workplaces
Article 31	**Right to Privacy:** Protects persons from unnecessary revelation of private information and infringement of communications.	Limits employer's unreasonable surveillance and mandates that any data collection must be justified and respect personal privacy.
Article 35	**Access to Information:** Grants citizens the right to information held by the State or others, required to protect any right/freedom.	Allows workers to request data collected about them and explanations of algorithmic decisions affecting their work or any other technology that affects their rights and freedoms.
Article 41	**Fair Labour Practices:** Guarantees every person the right to fair labour practices, including fair remuneration, joining a union, collective bargaining, and the right to strike.	Ensures core labour rights apply to all workers, including those on digital platforms, and protects against unfair labour practices that could be occasioned by digitalisation.
Article 27	**Equality and Freedom from Discrimination.** It guarantees every person the right to non-discrimination, either direct or indirect.	This could be the primary protection against any kind of discrimination emanating from the use of digital technology, including algorithmic bias. It allows workers to challenge automated systems, such as those for task allocation, pricing, or deactivation, if their outcomes disproportionately disadvantage them on the basis of protected grounds such as sex, age, or ethnic origin.

b) Data Protection Act, 2019 read together with the Data Protection (General) Regulations 2021 and the Registration of Data Controllers and Data Processors Regulations

The Data Protection Act (DPA) is Kenya's primary law governing the protection of personal data and giving effect to the constitutional right to privacy under *Article 31* of the Constitution. It is accompanied by the Data Protection (General) Regulations of 2021 herein referred to as General regulations. Their main purpose is to provide detailed, practical rules for implementing the obligations and rights set out in the main Act (DPA). They regulate how employers, businesses, government bodies, and third-party service providers collect, store, use, share, and delete workers' personal data.

The DPA also defines Sensitive Personal Data, which receives the highest level of legal protection. This includes a person's biometric data (fingerprints, facial images, iris scans); genetic data and health status; race, ethnic or social origin; marital or family details; sexual orientation; and property details, beliefs, and conscience.

Because workplaces increasingly rely on biometric attendance systems, digital HR platforms, CCTV, GPS tracking, and algorithmic decision-making, the DPA is essential for a. helping workers understand their rights, and b. for data processors and controllers, including employers, to understand their obligations when processing personal data.

Core principles relevant to workers in digitalized workplaces: The Act is built on key principles that all employers, businesses,[4] managers, including labour platforms, must follow as long as they process and control workers' data:

Lawfulness, Fairness, and Transparency (Sections 29-30 DPA and Orders 29, 30 and 36) of the Data Protection (General) Regulations, 2021

Personal data must be collected for legitimate reasons, used in a fair and transparent way, and workers must be informed about what data is being collected, why it is being collected, who will have access to it, whether it will be shared with third parties, security measures to protect such data, the consequences of where the data subject fails to provide any or part of the requested data and how long it will be stored.

It is important to note that, under the principle of transparency, a data controller/employer must inform employees of the nature, extent, and purpose of monitoring before it begins. This includes specifying what kind of data is being collected, for example, it could be data collected during the use of a computer, such as browsing history, etc., and how it will be used.

Workplace example:
A company introducing a biometric access system must clearly explain that fingerprints are needed for security, not for tracking attendance or monitoring employee productivity. This information must be shared during onboarding and made accessible.

Purpose Limitation (Section 25 (c) DPA, Regulation 31 of the General Regulation)

Employers and Businesses may collect data only for a specific, clearly defined purpose and may not repurpose it for unrelated uses.

Workplace example:
If fingerprints are collected for access control, they cannot later be used for timekeeping, disciplinary monitoring, or evaluating productivity without fresh consent and information on the purpose, etc.

Data Minimisation (Section 25(d) DPA, Regulation 33 General Regulations)

Only the minimum data necessary for the stated purpose should be collected.

Workplace example:
If an employer only needs two fingerprints for access, collecting all ten violates the principle of data minimisation.

Accuracy of Personal Data (Section 25(f) DPA, Regulation 34 General Regulations)

Employers must ensure that data held on workers is accurate and up to date. They should conduct regular data audits and correct or erase errors.

4 This analysis uses the terms "employer" and/or "businesses" not to imply that other types of data collectors and processors are exempt from these rules. These terms can be understood to refer to any person or institution that collects or processes data, including platforms and similar entities.

Storage Limitation (Section 25(g) DPA, Regulation 35 General Regulations)

Personal data must be deleted once it is no longer needed. Employers must have a clear retention schedule explaining how long data will be stored, why it is retained, and when and how it will be deleted.

Workplace example:
When a platform driver deactivates their account, financial records are kept only for tax purposes, GPS logs are kept only for customer support timeframes, and all other identifying data must be deleted when claim periods lapse.

Integrity and Confidentiality (Data Security) Section 29 (f) DPA

Employers must protect worker data against unauthorized access, loss, or hacking. Measures include encrypting biometric templates, implementing strict access controls, using secure storage systems, and conducting regular security audits.

Workplace example:
A company using fingerprint access encrypts all data, restricts access to authorized IT staff only, and continuously monitors for attempted breaches.

Consent and Workers' Autonomy (Section 30 (1) and Section 32 (2) DPA)

Consent must be freely given, specific, informed, and unambiguous. Workers must be able to withdraw consent without punishment.

Workplace example:
A logistics company implementing fingerprint entry must provide an alternative—such as a secure keycard and PIN—for workers who decline to give biometric consent. No worker should suffer loss of pay, demotion, or worse shifts for refusing.

Workers' Rights under the DPA (Section 26 DPA)

Workers have the right to be informed about how their data is used, to access, correct, and delete their personal data, to object to certain kinds of processing, to data portability, to be forgotten, and to lodge complaints with the Office of the Data Protection Commissioner (ODPC). These rights empower workers to challenge intrusive surveillance, unfair algorithmic decisions, or misuse of biometric data.

Employer Obligations under the DPA (Section 31 DPA Regulation 49 and 23 General Regulations)

Any employer or business that processes and/or controls workers data is required to register with the ODPC, create and implement a Data Protection Policy, conduct Data Protection Impact Assessments (DPIAs) when using high-risk systems (e.g., biometrics, automated decision-making, GPS tracking, behavioural profiling), ensure lawful contracts with third-party service providers, and ensure data retention and deletion procedures are in place.

Failure by a data controller or data processor, including an employer, to comply with their obligations under the Act and its associated Regulations triggers specific enforcement mechanisms and penalties. Specifically, Section 62 empowers the Data Commissioner to issue a Penalty Notice following a default on an Enforcement Notice, while Section 63 provides for administrative fines of up to KES 5,000,000 or 1% of the undertaking's annual turnover, whichever is lower. Beyond these administrative penalties, Section 73 establishes a general penalty for offenses where no specific fine is provided, which can include a fine of up to KES 3,000,000, an imprisonment term of up to ten years, or both. Furthermore, employers may face civil liability under Section 65, which entitles data subjects (workers) to seek compensation for both financial and non-financial distress resulting from such violations. The law provides for both administrative fines and criminal sanctions.

It is important to note that the Act and its General regulations only require that data controllers inform data subjects and seek consent for specific processing and give data subjects rights to access, know purposes, and object to processing of their data, ensuring transparency and control. This is more about informing and obtaining consent, and managing objections, rather than seeking views on the intended processing beforehand.

Workplace example:
Before implementing a fingerprint or facial recognition system, an employer must conduct a Data Protection Impact Assessment demonstrating why less intrusive methods (e.g., keycards, PINs) are insufficient and how the risks to workers' privacy will be mitigated.

Table 2

Table 2: Summary Articles on Data Protection Act, 2019

Principle / Right (Section)	Content	Relevance to Digitalised Workplaces
Lawfulness, Fairness & Transparency (S29-30) (Sections 29-30 DPA and Order 29, 30 and 36) of the Data Protection (General) Regulations, 2021	Data must be processed lawfully, fairly, and transparently. Data subjects must be informed about the processing.	Employers must clearly explain what data is collected by digital tools (e.g., trackers, biometrics) and why before the introduction of such technology that collects personal data.
Purpose Limitation (Section 25 (c)) DPA, Regulations 31 General Regulations	Data can only be collected for a specified, explicit purpose and not repurposed.	GPS data for route optimization cannot later be used for disciplinary action without fresh consent.
Data Minimisation (25(d) DPA, Regulation 33 General Regulations)	Only data that is adequate, relevant, and necessary for the purpose may be collected.	An employer cannot collect ten fingerprints if two suffice for a biometric system.
Storage Limitation (Section 25(g) DPA and Section 39 DPA)	Personal data must not be kept longer than necessary and must be deleted once the purpose expires.	Employers must define and follow strict retention schedules for biometric data, GPS logs, performance data, and monitoring records.
Integrity and Confidentiality (Data Security) (Section 29 (f) DPA)	Data must be secured against unauthorised access, loss, or destruction.	Mandates, for example, encryption and security for sensitive data such as biometrics or health information.
Rights of the Data Subject (Section 26 DPA)	Includes rights to access, correct, and delete personal data, and to object to processing.	Workers can challenge inaccurate performance data or demand deletion of data kept beyond its purpose.
Data Protection Impact Assessment – DPIA (Section 31 DPA, Regulation 49, General regulations)	Required before processing Data that is likely to pose a high risk to rights and freedoms.	Mandates an assessment before deploying high-risk[5] systems like facial recognition, automated decision-making.
Data Protection Policy (Regulation 23(1), General Regulations.	This regulation explicitly states that "A data controller or data processor shall develop, publish, and regularly update a policy reflecting their personal data handling practices".	It is important as it ensures that data processors and controllers / employers conduct internal due diligence and map all their data processing activities to promote accountability and compliance. The information on the policy could also be crucial to enforce rights under different laws for workers, but also to avert or mitigate any form of algorithmic discrimination
Registration with the Data Protection Commissioner (ODPC). (Section 18 DPA) Regulations 4 and 13, third schedule, Registration of Data Controllers and Data Processors Regulations	This requirement is mandatory for entities that have an annual turnover of Ksh 5,000,000 and above and have more than 10 employees. There is also a sector-specific mandate regardless of size and turnover for high risks sectors like Transport services firms (including those in online passenger hailing), financial services, Health administration and businesses wholly or mainly in direct marketing	This is important for digitised workplaces and is a tool to enforce accountability and transparency principles. This ensures that platforms, at a minimum, consider their obligations and put in place basic safeguards.

5 High risk has been defined as processing that is likely to result in a high risk to the rights and freedoms of individuals. This typically involves large-scale processing of sensitive data, automated decision-making or profiling that has a legal or similar effect, new technologies, systematic monitoring, and processing data of vulnerable individuals.

Principle / Right (Section)	Content	Relevance to Digitalised Workplaces
Failure to comply with the DPA and its accompanying regulations (Sections 62, 63, 73 and 65 of the DPA)	The Act provides for Criminal and Civil liability if any of the sections of the Act are violated.	The Enforcement sections empower workers to seek remedy whenever any of the rights under the Act and its accompanying regulations are violated. It also Creates a "Regulatory Safety Net" that allows workers to trigger state intervention when platforms fail to protect worker privacy.
Consent and Withdrawal of Consent (Section 32(2) DPA)	A data subject has the right to withdraw consent at any time. Where processing is based on consent, the data controller must stop processing once consent is withdrawn, unless another lawful basis applies.	Workers who originally agreed to biometric systems, GPS tracking, or monitoring tools have the right to later withdraw that consent without suffering retaliation, loss of pay, or disadvantage. Employers must provide alternative systems where consent is refused or withdrawn.
Retention and Deletion of Personal Data (Section 39 DPA)	Personal data may only be retained as long as reasonably necessary for the purpose for which it was collected. Data that is no longer required must be deleted, erased, anonymised, or pseudonymised.	Employers cannot keep historical GPS logs, biometric records, performance metrics, or monitoring data indefinitely. Once the purpose expires, worker data must be deleted according to a clear retention schedule.
Data Protection Policy Requirement (Regulation 23(1), General Regulations)	A data controller or processor must develop, publish, and regularly update a data protection policy outlining how personal data is handled.	Workers and their representatives can request this policy to understand what data is collected, how it is used, who accesses it, and how long it is kept. This is a key transparency and accountability tool in digital workplaces.

c) The Occupational Safety and Health Act (OSHA), 2007

The Occupational Safety and Health Act (OSHA) is Kenya's primary law for ensuring the safety, health, and welfare of all persons at work. Its broad definition of a "workplace" under *Section 3* covers *any* place where a person works that includes "any place, land, premises, location, vessel, or things, at, in, upon, or near which a worker is in the course of employment." This definition is broad in scope and could refer to permanent, temporary, remote, or even digital workplaces.

Key rights and obligations relevant to digitalised workplaces

The law imposes specific duties on employers and grants corresponding rights to workers, which are essential for mitigating the emerging risks of digital work. It is important to note that, at the time of writing, efforts are underway to reform the law to specifically address these emerging challenges, as the law is not fully cognizant of the diverse occupational challenges of the digitised world of work.

The Right to Protection Against Mental Strain (Section 76(2))

This is the most specific provision, requiring employers to adapt equipment and work tasks to the employee's ability, explicitly including protection against mental strain. This addresses psychosocial risks, such as stress, burnout, and fatigue, arising from digital engagement and surveillance.

Duty to Train and Inform (Section 6(2)(c))

Employers must provide workers with adequate information, instruction, training, and supervision on all work activities.

Workers can rely on this duty to request training on new digital systems, safe use of software tools, or managing stress and fatigue linked to digital work.

Information on Risks from New Technologies (Section 6(2)(f))

Employers are legally obliged to inform workers of risks arising from new technologies and any associated imminent danger.

Workers may therefore demand disclosure of psychosocial risks, for example from constant monitoring, algorithmic evaluation, or high digital workloads.

Research and Prevention Role of the Director (Section 24(4))

The Director of Occupational Safety and Health Services is empowered to conduct research on risks created by new technologies and recommend preventive measures.

Workers and unions can invoke this provision to seek official investigations into risks from digital systems and compel employers to follow recommended precautions.

Continuous Risk Assessment Duties (Section 6)

Employers must conduct risk assessments and adopt preventive and protective measures based on the findings.

In digital or remote work settings, this includes identifying psychosocial hazards, ergonomic risks (Section 76 (2)) from prolonged device use, and risks from digital surveillance systems.

Audit and Inspection (Section 11)

The law mandates regular safety and health audits. These can be used to examine digital work arrangements, remote setups, and technology-driven processes to ensure compliance with ergonomic and mental health protection standards.

Table 3

Table 3: Key Articles of the Occupational Safety and Health Act (OSHA), 2007

Section / Duty	Content	Relevance to Digitalised Workplaces
Duty to Train and Inform (Section 6)	Employers must provide adequate information, instruction, and training on work activities.	Workers can demand training on new software and on managing risks like stress from constant monitoring.
Information on Risks from New Tech (Section 6)	Employers must inform workers of risks arising from new technologies.	This could imply disclosure of psychosocial risks from algorithmic evaluation, digital surveillance, or any other risks related to technological tools used at work.
Risk Assessment (Section 6)	Employer must conduct a suitable and sufficient assessment of risks to safety and health, and on this basis, adopt preventative and protective measures to ensure all tools and machinery are safe and free of risk to health.	If the assessment conducted by the employer shows that there is a risk related to any technology, such as ergonomic injuries, mental strain, and surveillance stress, used at work, employers have an obligation to eliminate that risk or take protective measures.
Health and Safety Audits (Section 11)	The law mandates regular safety and health audits.	Audits must examine digital work arrangements, remote setups, and technology-driven processes.
Ergonomics at the Workplace (Section 76. (2))	The law mandates that the employer take the necessary steps to ensure that workstation equipment and work tasks protect employees from mental strain.	This is the most direct legal basis for protecting against any psychosocial risk at work. This is critical for workers who are interacting with digital technologies and platforms, like content moderators, whose work causes extreme mental strain that lead to psychosocial challenges.

d) Technical and Vocational Education and Training (TVET) Act, 2013 (Revised 2022), The Kenya National Qualifications Framework (KNQF) (General) Regulations, 2025

Coverage: The TVET Act applies across the entire labour market, regulating public and private TVET institutions, employers offering workplace training, and all workers or trainees engaged in technical, vocational, and digital skills development. The Kenya National Qualifications Framework Regulations set the standards, procedures, and quality assurance mechanisms for developing, accrediting, assessing, and recognising all national qualifications, ensuring consistency, comparability, and the mobility of learners and workers across education, training, and labour markets.

Recognition of Prior Learning

According to the KNQF Regulations (Regulations 19, 20, and 21), the TVET Act (Section 7 (1)(i)) mandates the Technical and Vocational Education and Training (TVET) Authority to recognise and equate qualifications obtained through informal pathways. Additionally, Section 43 provides a framework that enables the TVET Authority to assess and certify skills acquired through work experience. The KNQF Regulations also outline the Recognition of Prior Learning Framework under Regulations 19-21, which requires the state to promote the acknowledgment of skills, competencies, and experiential learning. Together, these laws create a legal foundation for the assessment, certification, and mapping of skills, especially those gained in the digital economy, into national qualification levels.

Why This Matters

Digitised workplaces in Kenya rely on skills such as data annotation, online content creation, and micro tasking. Many workers acquire these skills informally through online platforms or self-directed learning at work. The TVET Act and KNQF Regulations can serve as a basis for formally recognising these skills, enabling workers to obtain certification and qualifications. This recognition can help them access better job opportunities, negotiate fair wages, and ultimately build careers.

Workplace example: A Kenyan online freelancer (e.g., coder, digital designer, platform worker) can have their competencies evaluated, recognised, and certified under the RPL system (Recognition of Prior Learning), improving their employability, mobility, and bargaining power.

- **Worker empowerment:** Formal recognition of skills gained on digital platforms strengthens workers' ability to negotiate wages and access better opportunities.
- **Support for the digital economy:** Certification ensures that digital and tech-based skills are visible, portable, and valued in both formal and informal labour markets.

e) The Access to Information Act, 2016

The Act can promote transparency and accountability and give effect to the constitutional right of every Kenyan to access information held by public bodies, private entities, and persons. For workers, this means they can request information necessary to protect or exercise their rights, including in digitalized workplaces.

For private entities and persons under the Act, it empowers workers to invoke the right to use this law while protecting and exercising their rights and freedoms, which include the right to fair labour practices as discussed in the Constitution section.

Relevance for Workers in Digitalized Workplaces

- Workers may request policies, procedures, manuals, and decision-making rules used by employers, especially when work is managed through digital systems. This will apply for workers working in the public sector and have public entities as their employer, as for the private sector, one has to prove that they are exercising or protecting a right or freedom.
- Workers have the right to be given reasons for any decision made about them, including those generated or influenced by digital tools.

The Act (under section 3) can be used to demand transparency into algorithmic processes, such as the logic, inputs, and rules underlying automated or semi-automated decisions.

It supports the enforcement of other laws, including:

- OSH Act (e.g., accessing risk-assessment reports), and
- Data Protection Act (e.g., accessing policies on data handling and processing).
- Constitutional rights and freedoms.

Why it matters

The Act provides workers and their organisations with a critical tool that empowers workers to access information that is critical in accessing, exercising, and protecting their rights to fair labour practices while challenging the opacity that is facilitated by digital management tools while engaging in the world of work, while making organisations accountable for decisions driven by technology that affect the workers.

Note that section 5 of the Act gives examples of the kind of information that a person can request, for example, guidelines used by the entity in its dealings with the public or with corporate bodies, including the rules, regulations, instructions, manuals, and records held by the institution. However, it qualifies the information that a person can seek from public entities with the limitations set out in section 6 of the Act, which include, but are not limited to, undermining national security.

Table 4

Table 4: Key Articles in the Access to Information Act, 2016

Key Provision	Content	Relevance to Digitalised Workplaces
Right of Access to Information (Section 4)	Every citizen has the right to information held by the State or another person, where required to protect a right/freedom.	Workers can request internal manuals, algorithmic decision-making rules, and data policies to understand and challenge digital management practices.
Interpretation (Section 2)	"Information" includes all records held by a public entity or a private body, regardless of the form in which the information is stored, its source or the date of production.	This is essential to understand what information means for workers under this Act.
Disclosure of information by public entities (Section 5(a) (vi) Subject to Limitations (Section 6)	a public entity shall—(a)facilitate access to information held by such entity and which information may include— (vi)guidelines used by the entity in its dealings with the public or with corporate bodies, including the rules, regulations, instructions, manuals and records, held by it or under its control or used by its employees for discharging its functions; and	This provision is relevant for public servants and can also be interpreted as applying in the private sector to help workers understand the automated decision-making processes used in digital workplaces.
Disclosure of Information by public entities subject to section 6 limitations Section 5(1)(d)	provide to any person the reasons for any decision taken by it in relation to that person	This does so by giving workers the right to receive explanations for decisions that affect them
Right to Information (Section 4)	(1) Subject to this Act and any other written law, every citizen has the right of access to information held by— (a)the State; and (b)another person where that information is required for the exercise or protection of any right or fundamental freedom.	The section gives workers the right to know their data and systems, combat algorithmic bias, and ensure transparency in monitoring. It also provides a worker with the right to access information about a system or process itself, which is necessary to understand, for example, how their personal data was used to reach a decision.
Object and purpose of the Act (Section 3)	The object and purpose of this Act is to—(a) give effect to the right of access to information by citizens as provided under Article 35 of the Constitution;(b)provide a framework for public entities and private bodies to proactively disclose information that they hold and to provide information on request in line with the constitutional principles;(c)provide a framework to facilitate access to information held by private bodies in compliance with any right protected by the Constitution and any other law;(d)promote routine and systematic information disclosure by public entities and private bodies on constitutional principles relating to accountability, transparency and public participation and access to information.	This section explains the intent behind using this act as a tool to address opacity (lack of transparency) in digital workplaces. Reminding us that the law's primary goal is to empower citizens, and in this particular case, workers, to access information whenever their constitutional rights are engaged by the actions of an entity, whether in public or private

f) Employment Act 2007

The Employment Act is the main law that governs employment in Kenya and outlines the minimum terms and conditions of employment. It establishes fundamental standards for inclusion in contracts, wages, working hours, leave, maternity protection, and safeguards against discrimination and wrongful termination.

Section 5 outlines the legal framework against discrimination. This is important because it addresses the challenges faced by workers in digital workplaces, including both direct and indirect discrimination, and introduces the reverse burden of proof, key to challenging opaque algorithmic decisions and bias.

Section 5(3) prohibits an employer from discriminating, directly or indirectly, against an employee or prospective employee. On grounds that include race, colour, sex, language, religion, nationality, ethnic or social origin, disability, pregnancy, mental or physical condition, or HIV status. The prohibition applies to every aspect of the employment relationship, including recruitment, training, promotion, terms and conditions of employment, and termination of employment (which could include algorithmic deactivation cases). *Indirect discrimination* is essential for workers on digital platforms. It refers to policies or practices that appear neutral but have a disproportionately negative effect on people with a protected characteristic (e.g., an algorithm that favours data points historically associated with one gender).

Section 5(7) provides for the "reverse burden of proof," which is designed to help employees when evidence is controlled by their employer. This means the worker only needs to present facts that create a plausible inference or prima facie case. Basically, the facts should demonstrate that unfair treatment appears to be caused by discrimination, unless the employer can prove otherwise. The reverse burden of proof states that once an employee raises a plausible case, the employer (or platform) must prove they did not discriminate.

To break it down, these are the three basic facts an employee needs to prove:

1. You belong to a protected group
Examples

Sex / Gender example: Female ride	Is consistently allocated lower-paying tasks than male riders with similar ratings
Ethnic or Social Origin	Receives unfair reviews or being fired based on reports that mention your tribe, religion, or community.

2. You were profiled and treated unfairly
Examples

Deactivation / Firing	An employee experiences lower ratings due to societal biases from the community they come from, which eventually leads to deactivation.
Denial of Tasks	An employee was passed over for a better task or a promotion to a new contract.

3. Others were treated better
Examples

Deactivation	A driver from a different ethnic group who had a similar or even worse performance score was not deactivated.
Low-Value Tasks	A female rider and a male rider with the same rating, using the same type of vehicle, regularly get the higher-value corporate delivery orders.

The reverse burden helps workers, as platforms or employers must prove that the decision was NOT discriminatory and that the system or algorithm that made it was based on a genuine, non-discriminatory business reason.

Table 5

Table 5: Key sections under the Employment Act 2007 on Discrimination

Key Provision	Content	Relevance to Digitised Workplaces
Duty to Eliminate Discrimination (Section 5(2) & (3)	Prohibits an employer from discriminating directly or indirectly against an employee on various grounds (sex, disability, ethnic origin, etc.).	This could serve as a basis for challenging algorithmic or other forms of discrimination in digitised workplaces. The prohibition on indirect discrimination allows workers to challenge systems, such as automated systems (for task allocation, ratings, or pay), that disproportionately harm protected groups, even if the algorithm's code is facially neutral.
Scope of Practices (Section 5(3)(b))	Applies the prohibition to recruitment, training, promotion, terms and conditions of employment, and termination of employment.	Directly covers all automated processes. Algorithmic deactivation (automatic firing) is challenged under "termination of employment." Algorithmic wage-setting or task-assignment is challenged under the "terms and conditions of employment."
Reverse Burden of Proof (Section 5(7)	Requires the employer (digital platform) to prove that discrimination did not take place once the worker establishes a plausible inference of bias.	Forces algorithmic transparency. This is critical because the platform controls the code and data. It legally compels the platform to justify the algorithm's decisions with objective, non-discriminatory evidence, rather than forcing the worker to prove the code is biased.

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.

Questions for Workers Prior to the Introduction of New Digital Technologies

Checklist 1

Workers and their representatives should ask the following questions before a new digital technology is deployed in the workplace. The questions are grouped by theme for clarity.

Questions for Workers and Their Organisations	Legal Reference(s)
A: Skills, Recognition, and Employment	
1. How can we start the process of having our existing digital skills acquired through the kind of work we do in the digital economy formally recognised and certified (e.g., through Recognition of Prior Learning - RPL)	→ TVET Act, 2013; Kenya National Qualifications Framework Regulations
2. How can we use the TVET Act and KNQF recognition of prior learning framework to collectively negotiate for digital skills recognition in our workplace or platform?	→ TVET Act 2013; KNQF regulations
3. Can our platform agree to share workers' performance data that is relevant to support RPL assessments?	→ TVET Act 2013, KNQF regulations, Article 41 and 35 Constitution.
4. Does the deployment plan guarantee that workers with RPL-certified skills will receive equal consideration for promotions and new positions?	→ TVET Act, 2013
B: Health, Safety, and Ergonomics	
5. Has the employer conducted a Health and Safety audit and risk assessment to identify and mitigate hazards associated with this new technology?	→ Occupational Safety and Health Act (OSHA), 2007 (Section 11)
6. Will we receive adequate training on the safe and effective use of the technology, including all associated risks?	→ OSHA, 2007 (Sections 6(1)(c), 6(2)(c))
7. Has the employer formally informed all employees of the specific risks identified from this new technology?	→ OSHA, 2007 (Section 6(2)(f))
8. Have workstations, equipment, and tasks been ergonomically adapted to prevent physical strain or mental strain?	→ OSHA, 2007 (Section 76(2))
9. Will the employer provide any necessary new protective equipment (e.g., anti-glare screens) free of charge?	→ OSHA, 2007 (Section 6(2)(b))
C: Data Protection and Privacy	
10. Is the technology designed to collect only the minimum amount of personal data necessary for its stated purpose (Data Minimisation)?	→ Data Protection Act (DPA), 2019 (Section 25)
11. What is the lawful basis for collecting each type of data, and how will processing be made fair and transparent to workers?	→ Data Protection Act (DPA), 2019 (Section 25)
12. How long will the collected data be retained, and what is the process for its secure, automated deletion?	→ Data Protection Act (DPA), 2019 (Section 25)
13. Has a formal Data Protection Impact Assessment (DPIA) been completed, especially for high-risk technologies like biometrics or automated decision-making?	→ Data Protection Act (DPA), 2019 (Section 31)
14. If the technology involves automated decision-making (e.g., performance scoring), is there meaningful human oversight and a clear appeals process? If so, who is involved?	→ Data Protection Act (DPA), 2019 (Section 35)
15. Has the company demonstrated that the level of monitoring is necessary and proportionate, respecting our right to privacy?	→ Constitution of Kenya, 2010 (Article 31)
16. Have the workers been informed of the nature, extent, and purpose of the processing of their data, for example, monitoring, before it begins? This includes specifying what kind of data is being collected, for example, keystrokes, screenshots, or even browsing history, etc, and how it will be used.	→ Data Protection Act, Section 25 and Section 26
D: Transparency, Training, and Fundamental Rights	
17. How can we request internal manuals, procedures, or audit reports related to the security and functioning of this new system?	→ Access to Information Act, 2016
18. Does the introduction or operation of this technology infringe on our right to fair labour practices, including the rights to organise, bargain collectively, or strike?	→ Constitution of Kenya, 2010 (Article 41)
19. Can we access all information necessary to verify that the technology does not violate our constitutional and statutory rights?	→ Constitution of Kenya, 2010 (Article 35)
20. Have we been trained on the introduction of the risks associated with the digital tools that have been introduced in the workplace	→ Occupational Safety and Health Act, 2007 (Section 6(1)(d))

Checklist 2

Questions for Workers after the Deployment of Digital Technologies

Workers and their representatives should periodically ask the following questions to ensure ongoing compliance, safety, and fairness after a digital technology has been implemented.

Questions for Workers and Their Organisations	Legal Reference(s)
A: Data Protection and Privacy Compliance	
1. Has the purpose for which the technology collects and processes our data changed since it was first introduced?	→ Data Protection Act (DPA), 2019 (Purpose Limitation, Section 31)
2. If the purpose has changed, has management conducted a revised Data Protection Impact Assessment (DPIA) and obtained fresh consent if required?	→ Data Protection Act (DPA), 2019 (Sections 31 and 29)
3. Can we regularly access and review the personal data collected about us (e.g., performance metrics, location logs) to verify its accuracy?	→ Data Protection Act (DPA), 2019 (Right of Access, Section 26)
4. What is the process for requesting the correction or deletion of inaccurate or unlawfully processed data?	→ Data Protection Act (DPA), 2019 (Rights to Rectification and Deletion, Sections 26 and 27)
5. Has there been any data breach or unauthorized access to our personal data? If so, how were we informed and what remedial actions were taken?	→ Data Protection Act (DPA), 2019 (Integrity and Confidentiality, Section 40)
B: Health, Safety and Ergonomics (Ongoing)	
6. Has management conducted a new or revised health and safety risk assessment in response to issues that have emerged since the technology's deployment (e.g., increased stress, repetitive strain injuries)?	→ Occupational Safety and Health Act (OSHA), 2007 (Sections 6 and 11)
7. Are the training and safety procedures for the technology being updated regularly, especially after system upgrades or when new risks are identified?	→ Occupational Safety and Health Act (OSHA), 2007 (Section 6(1)(c))
8. Can we request a reassessment of our workstation ergonomics if we experience new physical or mental strain?	→ Occupational Safety and Health Act (OSHA), 2007 (Section 76)
C: Algorithmic Management and Performance Evaluation	
9. Are the algorithms or automated systems used for task allocation, performance scoring, or decision-making regularly audited for bias, errors, or fairness? If so, can we see this audit and, ideally, be part of the audit process?	→ Data Protection Act (DPA), 2019 (Automated Decision Making, Section 35); Constitution, Article 41 (Fair Labour Practices)
10. When an automated system makes a significant decision (e.g., flagging low performance, suspending an account), is there a transparent and timely human review and appeal process?	→ Data Protection Act (DPA), 2019 (Section 35)
11. Can we receive a meaningful explanation for decisions made by automated systems that affect our work status, pay, or assignments?	→ Access to Information Act, 2016; Constitution, Article 35
D: Worker Rights, Consultation and Fair Treatment	
12. How can we exercise our fundamental right to collective bargaining as workers?	→ Constitution, Article 41 (Right to Collective Bargaining)
13. Is data from monitoring systems (e.g., CCTV, GPS, keystroke logs) being used in disciplinary proceedings, and if so, is the evidence provided transparent and contestable?	→ Employment Act, 2007 (Fair Discipline); Data Protection Act, 2019 (Lawfulness and Fairness)
14. Has the technology led to unintended consequences, such as increased workload, unreasonable performance quotas, or a culture of constant surveillance that undermines trust?	→ Occupational Safety and Health Act (OSHA), 2007 (Psychosocial Risks); Constitution, Article 41 (Fair Labour Practices)
E: Transparency and Security	
15. Can we review the internal assessments related to the ongoing functioning and security of the digital system?	→ Access to Information Act, 2016
16. Are the third-party vendors who process our data (e.g., cloud providers, biometric system hosts) still compliant with data protection laws, and how is this being verified?	→ Data Protection Act (DPA), 2019 (Obligations of Data Processors, Section 42)

5.
Filling the Gaps – Bargaining Topic Suggestions

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

1. Limiting the Re-Purposing of Worker Data

If management introduces a technology that collects data for a specific purpose, a relevant bargaining topic could be:

→ Setting strict limitations on data processing: For example, negotiate that data collected from a vehicle's GPS to optimize fuel efficiency and delivery routes cannot be repurposed to monitor a driver's speed for disciplinary action or to set unrealistic delivery time targets.

2. Restricting Data Collection on Personal Devices and Time

If workers are required to use a mobile app for clocking in and out, managing schedules, or tasks, workers could bargain for:

→ Data limitation: The app's permissions are strictly limited, and it cannot access the phone's microphone, camera, or other sensors. Furthermore, the app must be programmed to cease all data collection outside of the employee's officially scheduled working hours.

→ Rights of Access and Contestation: That the worker and their union representative have the right to receive a full, clear copy of the raw data if it is used to make a claim about conduct (e.g., taking long breaks). This data must be provided in a simple, readable format to allow the worker to challenge its accuracy or context.

3. Ensuring Genuine Consultation and Joint Oversight of Risks

If management conducts a risk assessment related to new technology, workers could bargain for:

→ The right to be formally consulted as part of the risk assessment team, not just informed after the fact.

→ Access at all times to the full risk assessment report, including all identified psychosocial risks (like stress from constant monitoring) and not just physical hazards.

→ The right to joint consultation on the specific remedies chosen to mitigate identified risks, and to have scheduled follow-up meetings to review the effectiveness of these measures and make adjustments. This could be incorporated into OSH committees.

4. Negotiating Transparency and Human Review in Algorithmic Management

If performance, task allocation, or pay is managed by an automated system, a relevant bargaining topic could be:

→ **The right to a meaningful explanation**: For example, a ride-hailing driver must be able to receive a clear breakdown of how their fare was calculated and the factors that led to a low performance rating.

→ **The right to a human appeal process:** Negotiate that no worker can be suspended or have their account deactivated based solely on an automated alert. Every significant decision must be reviewed by a human manager, and the worker must have the right to a fair hearing to contest the decision.

→ **The right to data access and workflow transparency:** Negotiate for workers and their representatives to have full access to the raw data and parameters used in decision-making. This includes visibility into the workflow process, i.e. how tasks are funnelled, prioritised, and valued to ensure that the "logic" of the algorithm does not hide systemic biases or unfair labour practices.

→ **Pre-deployment "white box[6]" testing:** Establish a protocol where any new algorithmic system or significant update must undergo "white box" testing before it is deployed. This allows for a transparent audit of the internal code and decision-making logic to identify potential errors or discriminatory outcomes in a "sandbox" environment, rather than testing live on workers' livelihoods.

5. Establishing Boundaries on Surveillance and Monitoring

If the workplace uses CCTV, biometric systems, or computer monitoring software, workers could bargain for:

→ Proportionality and purpose limitation: For instance, negotiate that continuous keystroke logging or screen capture is prohibited, and that any monitoring must be sample based. Furthermore, agree that CCTV cameras will not be installed in break rooms, toilets, or other areas where workers have a reasonable expectation of privacy and will not interfere with their right to freedom of association and any other fundamental right.

6. Securing the Right to Skill Development and Recognition

If new technology changes job roles or creates new ones, a relevant bargaining topic could be:

→ Guaranteed training and upskilling: Negotiate a company-funded training plan to ensure all affected workers can transition into new roles, with pay protected during training.

→ Formal recognition of acquired skills: Bargain that any new digital skills learned on the job are formally certified and recorded in the worker's record, and that this certification is linked to career advancement opportunities and remuneration.

7. Addressing Digital Skills Gaps

If necessary for the employer to ensure that workers and managers have the necessary skills and knowledge to operate and use the digital system, relevant bargaining topics could include:

→ Mandatory training before deployment of new technologies.

→ On-going capacity-building and refresher training.

→ Equal access to training opportunities.

→ Joint oversight committee on digitalisation.

6 The "White box testing" signals that workers are demanding to see the internal workings of the system. It moves the conversation from "trust us; it works" to "show us the logic."

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!

The digitalisation of Kenya's workplaces presents a complex duality: it offers significant opportunities for efficiency, service delivery, and the creation of employment, particularly for young people, but simultaneously introduces profound challenges to worker rights, dignity, and fair labour practices. Despite the rapid transitions toward digitalised workplaces, a review of available collective bargaining language, at the time of writing this report, shows no negotiated clauses that explicitly address digitalisation, including issues such as algorithmic management, data-driven performance monitoring, workplace surveillance, digital skill requirements or protections in remote and on digital labour platforms. This critical gap underscores the urgent need for worker organising and proactive bargaining frameworks that address the challenges that are brought by digital tools.

This report has examined the state of play, analysing both the technologies in use and the existing legal framework that workers can use to invoke rights and protections. The central reflection is that while Kenya's existing constitutional foundation is robust and provides significant formal rights, a substantial implementation and enforcement gap prevents these rights from being fully realised, leaving workers inadequately protected in practice, particularly in how the constitutional principles are applied in digitalised workplaces. This creates a clear call for legal reforms, especially labour-law reforms that respond to the challenges of digitised work, while also recognising the opportunities existing laws already provide for asserting protections and rights.

Sufficiency of Existing Rights: Strong on Paper

On paper, Kenyan workers are not powerless. The Constitution of 2010, particularly Articles 31 (privacy), 35 (access to information), and 41 (fair labour practices), provide a powerful bedrock. The Data Protection Act (2019) is a comprehensive law that, if fully applied, would strictly regulate workplace surveillance, biometric data collection, and algorithmic decision-making. Furthermore, the Occupational Safety and Health Act (2007) has a broad definition of the "workplace" and "risk" to encompass psychosocial harms from digital monitoring and the ergonomic strains of digital work.

Having said this, there is not only an absence of regulations in helping realise rights as intended in the constitution but a need for the enforcement of existing rights, which is mainly as a result of the power imbalance and reality of workers that prevent workers from invoking such rights, especially workers in precarious platform work and non-unionized sectors. The lack of knowledge, resources, and bargaining power often leads to violations but gives an opportunity for workers and organisations to reflect on the opportunities and lack of protections thereof in realising decent work in a digitalized world of work.

Critical Gaps in the Current Landscape

Several critical gaps persist:

1. **The Awareness and Power Gap:** Many workers and frontline managers are unaware of the provisions of the DPA or OSHA and other laws in the context of digital tools. This knowledge asymmetry allows for the introduction of systems without the requisite transparency, impact assessments, or less intrusive alternatives.

2. **The Accountability Gap for Algorithms**: While the DPA provides a right to explanation for automated decisions, this is difficult to enforce against multinational platform companies whose algorithms are "black boxes." There is a lack of specific regulation mandating algorithmic transparency and auditability in employment contexts.

3. **The Collective Rights Gap for Non-Standard Workers:** The classification of platform workers as "independent contractors" creates a legal fiction that strips them of the core collective bargaining rights guaranteed under Article 41. This denies them a meaningful voice in shaping the very algorithms that control their livelihoods.

4. **The Enforcement Gap**: The Office of the Data Protection Commissioner (ODPC) and other regulatory bodies are still building capacity. Proactive enforcement in workplaces is limited, placing the burden of reporting violations on individual workers, which is often impractical due to fear of reprisal.

Suggested Ways Forward

Addressing these challenges requires a coordinated strategy that leverages existing tools while building new structures through building workers' voice and power.

1. **Application of Existing Laws:** The most immediate and powerful path is to insist on the application of existing laws. This includes:

→ **Utilising the DPA complaints mechanisms and the DPA aggressively**: This includes utilising the DPA complaints mechanisms effectively. This is for breaches involving, for example, the filing of complaints with the ODPC against employers who deploy biometric systems without conducting DPIAs, repurpose data unlawfully, or lack a lawful basis for processing.

→ **Invoking the Constitution and the Employment Act**: Proactively challenge unfair labour practices and discriminatory conduct under Article 27 (Equality) and Article 41 (Labour Relations) of the Constitution. This includes utilising section 5 of the Employment Act to contest both direct and indirect discrimination in digitised workplaces, such as algorithmic biases that use proxies (like GPS location or behavioural data) to unfairly limit a worker's right to fair remuneration or their freedom of association.

→ **Enforce OSHA's mandate**: Demand that risk assessments for new technologies include, amongst others, psychosocial risks like stress from surveillance and unsustainable productivity quotas.

2. **New Labour Market Agreements and Policies:** Existing laws provide the floor, not the ceiling. Collective bargaining is the key mechanism to build upon them. The path forward must include:

→ Negotiating CBA Digitalisation Agreements that contain a digitisation aspect, including the revival of the national sectoral bargaining: Sector-wide and company-specific agreements that codify rights beyond the law, such as the "right to disconnect," strict limits on data re-purposing, and joint union-management technology oversight committees. To also ensure minimum standards in the digitised world of work, it is important for workers and their organisations to revive the national sectoral agreements to ensure minimum standards for workers in different sectors, for example, in data labelling, where workers are isolated. This could also present an opportunity for developing a national regulation for different sectors of the application of digital monitoring or devices in different employment contexts.

3. **Targeted Legislative and Policy Reforms:** In the medium term, specific legal clarifications are needed:

→ **Fair labour practices for all workers**. Legislative intervention is necessary to ensure that all workers, regardless of their employment relationship, have the rights as provided for in the Constitution, which ensure fundamental freedoms and rights at work, in particular freedom of association and collectively bargaining.

→ **Strengthen Provisions on Algorithmic Management**: Future amendments to the DPA or new legislation could introduce mandatory algorithmic impact assessments and a right to human review for all significant automated decisions in employment.

→ **Ensure that existing labour laws are reformed and grounded** on the reality of workers' digital inequalities and include safeguards on issues like the right to disconnect, sexual harassment policies, psychological wellbeing, and other aspects in a digitised world of work for all workers and various forms of misconduct.

7.
Annex – Links to the Laws and Agreements Covered

This annex contains the exact text of the key legal articles and sections referenced throughout this country report, providing a direct source for the rights and obligations discussed.

- **The Constitution of Kenya, 2010**
  Official link https://new.kenyalaw.org/akn/ke/act/2010/constitution/eng@2010-09-03

- **Data Protection Act, No. 24 of 2019**
  Official link: https://new.kenyalaw.org/akn/ke/act/2019/24/eng@2022-12-31

- **The Data Protection (General) Regulations, 2021 Legal Notice 263 of 2021**
  Official link: https://new.kenyalaw.org/akn/ke/act/ln/2021/263/eng@2022-01-14#part_IV__sec_23

- **Occupational Safety and Health Act, No. 15 of 2007**
  Official link: https://new.kenyalaw.org/akn/ke/act/2007/15/eng@2022-12-31

- **Technical and Vocational Education and Training (TVET) Act, 2013 (Revised 2022)**
  Official link: https://new.kenyalaw.org/akn/ke/act/2013/29/eng@2022-12-31
  Link to the Technical and Vocational Education and Training Authority (TVETA): https://www.tveta.go.ke/

- The Kenya National Qualifications Framework (General) Regulations, 2025
  Official link: https://knqa.go.ke/wp-content/uploads/2024/07/FINAL_THE-KENYA-NATIONAL-QUALIFICATIONS-FRAMEWORK-GENERAL-REGULATIONS-2025-FINAL-1.pdf

- **Access to Information Act, No. 31 of 2016**
  Official link: https://new.kenyalaw.org/akn/ke/act/2016/31/eng@2022-12-31

- **Employment Act 2007**
  Official link: https://kenyalaw.org/akn/ke/act/2007/11/eng@2024-04-26

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.

G

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

Jacqueline Wambui Wamai
Regional Coordinator, Sub-Saharan Africa
International Lawyers Assisting Workers (ILAW) Network

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