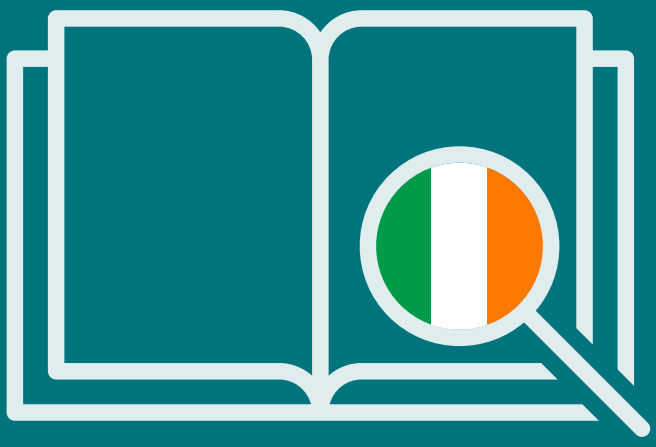
STUDY

Marta Lasek-Markey
April 2026

Negotiating Digitalised Workplaces

Rights and Obligations, Ireland



Friedrich Ebert Stiftung

Imprint

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

Publishing department
Division for International Cooperation |
Global and European Policy

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

Contact
Blanka Balfer
blanka.balfer@fes.de

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

April 2026

ISBN 978-3-98628-859-4

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

Friedrich Ebert Stiftung

Marta Lasek-Markey
April 2026

Negotiating Digitalised Workplaces

Rights and Obligations, Ireland

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 PSIs Digital Bargaining Hub, the vast majority are still not. To support unions in their negotiations with management, this series of reports brings to light what rights workers have when digital systems are deployed at work and what obligations management have in relation to the workers. The reports provide ready-to-use checklists of questions, and collective bargaining suggestions to bridge legal gaps.

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

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

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

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

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

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

1.
Introduction – Technology at Work Is a Labour Issue

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

These technologies are often presented as technical tools to improve efficiency or service quality. But for workers, they change how work is organised, monitored, evaluated, and controlled. This report is designed to help workers and unions understand which laws already apply, which questions they have a right to ask based on those laws, and how to use those rights when digital technologies are introduced or used at work. It also shows how collective bargaining can be used to address gaps that existing law does not fully regulate.

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

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

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

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

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

How to use this country report

This report is written for workers, union representatives, and negotiators in Ireland, where digital technologies are expanding rapidly across public and private sectors. Despite a strong regulatory framework—particularly in data protection, occupational safety and health, and information and consultation—gaps exist and enforcement of current legal provisions must be improved.

The report helps unions move from reactive enforcement to preventive engagement. It explains how Irish and EU law applies to workplace surveillance, algorithmic management, and AI systems, and how these rules can be used strategically in discussions with management.

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 Ireland. 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 technology 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 Irish Workplaces

According to statistics gathered by the Central Statistics Office (CSO), as of 2024 15% of all enterprises in Ireland used AI technologies "in some capacity". In 'PwC 2025 GenAI Business Leaders Survey', 98% of Irish businesses declared having started using AI. Many employers, including in the public sector, have introduced Microsoft Co-Pilot to employees, with prominent examples reported by Microsoft including the AIB Bank and the electricity supplier ESB. The types of digital technologies used to monitor workers and process their personal data include keystroke logging, phone and login data, emotion-detecting badges, GPS tracking, as well as CCTV monitoring. The prevalence of these methods was uncertain, and this will also be impacted once the recently adopted EU AI Act fully comes into effect in employment matters.

The use of technology in the workplace was evidenced in a notable report by the Irish Financial Services Union on the employee experiences of technological surveillance. According to a survey conducted with over one thousand respondents in 2021, when many were working from home due to the COVID-19 pandemic, 38% reported that their office computer was being monitored, while 20% had their computer use monitored also at home. One-third of the respondents indicated that they used personal identification mechanisms processing personal data to access work systems, such as facial recognition, fingerprints or eye scans. 30% of the survey participants also had their phone use monitored. Importantly, many of the surveyed workers were not aware whether they were being monitored or not. One specific example of a third-party software was Genesis, described by one of the interviewees as a system that tracked employee activity, including login/logout times, breaks, call and email volumes, and overall availability at the desk, and provided detailed statistics on daily performance and presence.

The Irish Data Protection Commission (DPC) has also published a case study describing how data derived from **swipe cards** documenting an employee's entrances and exits from the office was being unlawfully used as evidence of their poor timekeeping in a disciplinary action. However, the employer had not informed the employees that swipe card data would be used for disciplinary or time-keeping purposes; it was supposedly collected only for access and security purposes. The DPC held that because the purpose of using the data for discipline was not disclosed in advance, the processing was in breach of the GDPR requirements.

One well-documented example of technology being used for worker surveillance in Ireland is the use of **GPS tracking devices**. This was addressed in a recent case *Barry Naughton v Protum Services* [2024] brought before the Irish Workplace Relations Commission (WRC). The applicant, who was a builder, was dismissed after his employer accused him of misusing a company van and tampering with a GPS tracker that had been secretly installed. The tracker monitored his movements, including outside work hours, without his prior knowledge or consent. The WRC found that, while some concerns may have been legitimate, the employer's failure to inform the worker about the surveillance rendered the dismissal unfair. Another use case of mandatory wearable location-tracking technologies for employee management was reported in research among the members of An Garda Síochána, Ireland's police force. Gardaí raised concerns that GPS trackers were being used to monitor their movements beyond operational needs, creating a sense of constant surveillance.

The use of digital technologies for managing workers is also becoming increasingly popular in the healthcare sector, including through digital platforms, as has been revealed in a recent study conducted by the Irish trade union SIPTU. Thus, nursing agencies are reported to have adopted digital scheduling software with features **like online scheduling, payroll integration and shift swapping**. Note that the obligations of digital labour platform operators will change following the implementation of the EU Platform Workers Directive.

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

In Ireland, the relevant Legislation includes:

- → GDPR (General Data Protection Regulation *(EU) 2016/679*), read together with the Data Protection Act 2018
- → The EU AI Act (*Regulation (EU) 2024/1689*)
- → Safety, Health and Welfare at Work Act 2005, read with Safety, Health and Welfare at Work (General Application) Regulations 2007
- → Employment Equality Acts 1998–2015
- → Terms of Employment (Information) Act 1994, as amended by the European Union (Transparent and Predictable Working Conditions) Regulations 2022
- → Organisation of Working Time Act 1997
- → The Employees (Provision of Information and Consultation) Act 2006
- → European Union (Award of Public Authority Contracts) Regulations 2016 and additional legislation
- → Protected Disclosures Act 2014
- → EU Platform Workers Directive 2024/2831
- → FSU Agreement

Below, we set out the key rights you already have when management decides to introduce or use digital technology at work. We do this law by law, pointing you directly to the specific provisions you need to know. Alongside your rights, we also highlight management's legal obligations to you, including duties to consult, ensure system transparency, conduct risk assessments, and more.

Then, in the next section, we bring this together into two practical sets of questions you can use to hold management to account. The first set covers questions to ask *before* a new digital technology is introduced. The second set covers your *ongoing rights* once the technology is in use. Every question is grounded in existing laws and/or collective agreements. Where management is reluctant to engage or provide answers, we reference the exact legal provisions you can rely on.

GDPR (General Data Protection Regulation (EU) 2016/679) read together with the Data Protection Act 2018

- → **Art. 5**
  Sets out core data-protection principles
- → **Art. 6**
  Defines when processing is lawful
- → **Art. 9**
  Prohibits processing of special categories of data
- → **Art. 12**
  Requires controllers to provide transparent information and communications
- → **Art. 13**
  Specifies what information must be given when personal data are collected directly from the individual
- → **Art. 14**
  Specifies what information must be given when personal data are obtained from other sources
- → **Art. 22**
  Gives individuals the right not to be subject to decisions based solely on automated processing
- → **Art. 35**
  Requires a Data Protection Impact Assessment (DPIA) for high-risk processing and 35.9 says that in our case the employer shall, where appropriate, seek the views of the workers and/or the union representative
- → **Art. 80**
  Allows individuals to mandate qualified non-profit bodies to act on their behalf. In workplaces this mandate can be given to the union representative
- → **Art. 88**
  Allows Member States to adopt specific rules for employee data processing through law and/or collective agreements
- → **Data Protection Act 2018, s.4**
  Prohibits employers from requiring applicants or employees to exercise access rights (e.g., request their own data) or provide their access-request results

The EU's GDPR has been in effect since 2018 replacing in Ireland the Data Protection Acts 1988 and 2003 (which still applies to situations that had occurred before 2018). It generally applies to the processing of personal data within the EU, imposing enhanced responsibilities on data controllers and processors while strengthening the rights and protections of data subjects.

Under Article 5 GDPR, employers must adhere to key data protection principles, including lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality, and accountability. These principles guide how personal data is collected, used, stored, and shared throughout the employment lifecycle.

Employers must also identify a lawful basis for processing personal data in accordance with Article 6 GDPR. This may include situations where processing is necessary for the performance of a contract, compliance with a legal obligation, the protection of vital interests, legitimate interests pursued by the employer, or, in limited cases, consent. When handling special categories of data, such as health information (for instance, details of medical leave, ergonomic assessments, or reasonable adjustment requests), employers must also meet one of the specific conditions set out under Article 9 GDPR.

Chapter 3 GDPR is also very important for workers' rights. Article 12 requires employers – as data controllers – to provide information to employees in a clear, accessible way and to facilitate the exercise of their rights. Article 13 sets out the information that must be given to employees when their personal data is collected directly from them, including the purposes, legal basis, recipients, storage period, rights etc. The same applies when data is obtained from third parties. In accordance with Article 14, if an employer gathers information about a worker from someone else, such as background checks, references, or publicly available sources, they must inform the worker.

Furthermore, Article 22 GDPR restricts decisions based solely on automated processing, including profiling, where such decisions have legal or significant effects on individuals. This means that when employers use AI-driven tools in recruitment, performance evaluation, or other HR processes, they must ensure that human oversight and judgment remain part of the decision-making process.

Article 35 GDPR requires employers as data controllers to conduct a Data Protection Impact Assessment (DPIA) before carrying out any type of processing that is likely to pose a high risk to individuals' rights and freedoms, especially when new technologies are involved. It specifies situations where a DPIA is mandatory, such as large-scale processing of sensitive data, extensive automated decision-making, or large-scale monitoring. Crucially, workers or their representatives have a right to be consulted on the intended processing unless precluded by important commercial or public interests or the security of processing operations.

Article 80 GDPR allows data subjects such as workers to appoint a qualified non-profit organisation to act on their behalf in data-protection matters such as lodging complaints, challenging decisions, or seeking compensation.

Finally, Article 88 allows the Member States to provide for more specific rules in respect of the processing of employees' personal data in the employment context. In Ireland this is done through the Data Protection Act 2018 (DPA) which, in Section 4, prohibits employers and prospective employers from requiring an individual to make, or provide data obtained through a data subject access request.

The EU AI Act (Regulation (EU) 2024/1689)

- → **Art. 4**
  Requires providers and deployers to ensure sufficient AI literacy and training for staff
- → **Art. 5**
  Bans certain AI uses, including manipulative or subliminal techniques, exploitation of vulnerabilities and emotion inference at work
- → **Art. 9**
  Requires a continuous risk-management process for high-risk AI, including risks to health, safety and fundamental rights
- → **Art. 14**
  High-risk AI must be designed and used with effective human oversight
- → **Art. 27**
  Requires certain deployers of high-risk AI to assess and document the system's impact on fundamental rights before first use
- → **Annex III (1)**
  Lists high-risk AI in biometrics, including remote biometric identification, biometric categorisation by sensitive traits, and emotion-recognition
- → **Annex III (3)**
  Lists high-risk AI used for access to education and vocational training
- → **Annex III (4)**
  Lists high-risk AI used for recruitment and selection, and for decisions on working conditions, promotion, termination, task allocation, and performance evaluation

In 2024, the EU adopted a risk-based framework for regulating AI across its Member States, including Ireland, which draws inspiration from the existing product safety laws. As a result, the legislation categorises AI systems based on different levels of risk. AI systems deemed to pose an unacceptable risk, such as the use of AI to infer a person's emotions in the workplace, as well as the use of AI to predict a person's trade union membership based on biometric categorisation, are prohibited by Article 5(1).

In contrast, high-risk AI systems are permitted but must comply with stringent mandatory requirements. AI in the context of employment and workforce management is considered one of the high-risk areas as per Article 6(2) read together with Annex III to the Act. This includes AI systems intended to be used for:

- → AI systems used in recruitment processes, such as those that target job advertisements, screen applications, or assess candidates; and
- → AI systems used to make decisions about employment conditions, including promotions, task allocation, dismissals, or to monitor and evaluate employee performance or behaviour, particularly based on individual traits or conduct.

As "work-related contractual relationship" is in principle a wider concept than an employment relationship, it could also capture arrangements with platform workers, self-employed consultants and staff supplied via employment agencies.

This part of the AI Act will become fully effective in August 2026. From then on, employers using high-risk AI technologies will have to meet additional obligations, such as following the provider's instructions, appointing qualified staff to manage the system, ensuring the quality of input data, monitoring how the system performs, and keeping detailed records of its operation. Employers deploying high-risk AI in the public sector and those private employers providing public services will also carry out a Fundamental Rights Impact Assessment to identify specific risks the system could pose to the affected individuals or groups, contingency plans and human oversight measures.

Another important provision of the AI Act is Article 4 on AI literacy. It requires employers who provide or deploy AI systems to ensure that employees have enough understanding of how those systems work and how to use them safely and appropriately. It means workers should receive training suited to their role, experience, and the specific AI tools they interact with, helping them avoid misuse, identify risks, and understand the impact of the AI systems on themselves or others. This Article also distinguishes between "operation" as opposed to "use" of AI systems. While the AI Act itself does not define the term "operation", it might imply management should provide the workers and managers involved with the necessary competencies to govern these AI systems.

In Ireland, the EU AI Act will be enforced by many government bodies and agencies, with those most relevant to workers being the Workplace Relations Commission and the Data Protection Commission.

Safety, Health and Welfare at Work Act 2005, read together with the Safety, Health and Welfare at Work (General Application) Regulations 2007

- → **Section 19**
  Requires employers to carry out a risk assessment
- → **Section 20**
  Requires a written safety statement based on the risk assessment
- → **Section 26**
  Obligates employers to consult employees and safety representatives on health and safety measures, risk assessments, training etc
- → **Regulations 2007, Schedule 4**
  Prohibits the use of any monitoring or checking functions within software involving screens without the employee's knowledge

The Safety, Health and Welfare at Work Act 2005 (SHWW) establishes a general legal framework for occupational health and safety in Ireland aligning national law with key EU directives, including the so-called OSH Framework Directive 89/391/EEC. The 2005 Act sets out broad duties for employers, employees, designers, and suppliers to ensure safe and healthy workplaces. Under Section 19 of the Act, all employers are obliged to carry out a health & safety impact assessment and to review it where there has been any significant change, e.g. a new technology introduced. Under Section 26(1), employers have a duty to consult with employees, their safety representatives or both, on the impact assessment and the resulting safety statement, as well as on the planning and introduction of any new technologies and on any proposed measures which may substantially affect employee safety, health and welfare.

The Act is supported by detailed regulations, notably the Safety, Health and Welfare at Work (General Application) Regulations 2007 which implement relevant EU legislation such as the Display Screen Equipment Directive 90/270/EEC. Specifically, Article 3 of Schedule 4 to the 2007 Regulations requires employers to ensure that any software used by employees is appropriate for the task, user-friendly, and suited to their level of experience. Crucially, it prohibits the use of any monitoring or checking functions within that software without the employee's knowledge, thereby establishing a clear transparency requirement for digital employee surveillance.

The 2007 Regulations also confer upon employers providing digital equipment to employees a duty to plan the employees' activities in such a way that daily work in front of the screen is periodically interrupted by breaks or changes of activity. The same rules apply when employees are working from home. The Health and Safety Authority has issued 'Occupational Health and Safety Guidance on Remote Working' according to which the occupational health and safety requirements applicable to employers remain the same where the workplace is remote.

Employment Equality Acts 1998–2015, as amended

- → **Section 6**
  Defines discrimination as less favourable treatment based on nine protected grounds
- → **Section 8**
  Prohibits discrimination specifically in employment
- → **Section 14**
  Makes it an offence to procure or attempt to procure another person to engage in unlawful discrimination or victimisation
- → **Section 76**
  Allows a person who suspects discrimination to obtain material (non-confidential) information relevant to a potential complaint
- → **Section 85A**
  Sets out the rules on the burden of proof in discrimination cases

The Employment Equality Acts prohibit employment-related discrimination, whether direct or indirect. It implements the EU non-discrimination law including the Framework Directive 2000/78/EC, the Racial Equality Directive 2000/43/EC and the Gender Recast Directive 2006/54/EC. In Ireland, however, protection from discrimination extends over nine grounds – outside the EU-protected grounds of gender, age, disability, race, sexual orientation and religion, it also covers protected grounds such as civil status, family status and membership of the traveller community.

Section 14 of the Acts prohibits victimisation to prevent the employer from penalising an employee for making a discrimination complaint.

Under Section 15, employers are also responsible for acts of discrimination carried out by their employees or by third parties (such as clients, contractors, or other business contacts) unless they show that they took all reasonably practicable steps to prevent such discrimination from occurring.

To prove direct discrimination, i.e. unfair treatment due to one of the protected characteristics, it is essential to find a comparator who is in a similar situation yet does not share the protected characteristic of the claimant. For example, an algorithm screening job applicants that automatically downgrades CVs from candidates with foreign-sounding names could lead to direct discrimination on the grounds of race or ethnic origin. Conversely, indirect discrimination, i.e. a rule, requirement, or practice that seems neutral and fair, but it places people belonging to one of the nine protected groups at a particular disadvantage, may sometimes be allowed.

Under Section 85A of the Acts it is the complainant who is responsible for establishing the primary facts in discrimination cases and only after this has been established does the burden of proof shift onto the (prospective) employer. To facilitate that, Section 76 gives a person who believes they have been discriminated against, victimised, or treated unfairly under the Employment Equality Acts the right to seek material information, excluding confidential personal data, from the other party (usually the employer) before deciding whether to make a formal complaint. Furthermore, if unions have any indication of discrimination, this can also trigger the reversed burden of proof.

Note that the Employment Equality Acts are currently under review, with a revision implementing the EU Pay Transparency Directive 2023/970 underway, and recognition of the compounding effect of discrimination being considered.

To ensure compliance with the Employment Equality Acts, employers using AI or algorithmic management in recruitment or other HR processes have a duty to ensure that these tools operate in a fair, transparent, and non-discriminatory manner. Furthermore, in line with emerging expectations around AI transparency combined with pay transparency, employers should be able to explain how automated decisions are made and demonstrate that these systems do not reinforce existing inequalities, for example those reflected in gender pay gaps.

Terms of Employment (Information) Act 1994, as amended by the European Union (Transparent and Predictable Working Conditions) Regulations 2022

→ **Section 3**
Requires employers to give employees written statements of their core terms

→ **Section 5**
Employers must notify employees in writing of any changes to the terms stated in their written statement

→ **Section 6G**
Sets out rules on employee training

The Terms of Employment (Information) Act 1994 requires employers in Ireland to provide employees with clear, written details of the main terms and conditions of their employment. Its purpose is to ensure transparency and certainty in the employment relationship by obliging employers to give workers information such as job title, pay, hours of work, and notice periods. The Act sets out when and how this information must be given, and forms part of the broader framework of Irish employment rights legislation.

In 2022, the Act underwent a significant revision by the European Union (Transparent and Predictable Working Conditions) Regulations 2022 which implement the EU Directive 2019/1152 on transparent and predictable working conditions. The Regulations have also introduced changes to other Irish legislation such as the Organisation of Working Time Act 1997.

Under Section 3 of the Act, as amended by the 2022 Regulations, employers must give workers clear, written terms early on, setting out core information such as place of work, work hours, and notice periods, and they must notify employees of any changes before they take effect. This also applies where the work pattern of an employee is entirely or mostly unpredictable. Thus, any automated scheduling, monitoring, or decision logic that affects hours, shift assignments, or remote/flexible working must be transparently captured in those terms and communicated in advance. While the information obligations apply across all forms of work, they are particularly relevant in contexts where AI systems or algorithmic management tools influence scheduling, task allocation, or performance monitoring.

The Regulations have also limited the use of unpredictable or "on-demand" scheduling. For instance, if an employer wants to assign work outside the agreed "reference hours and days," the worker must receive notice (or may refuse) without penalty in certain cases. In practice, algorithmic systems that dynamically alter shifts or allocate tasks must respect these predictability limits and provide workers with fair notice.

Furthermore, Section 6G of the Act, inserted by the 2022 Regulations, ensures that any legally required training, such as forthcoming AI literacy training under Article 4 of the EU AI Act, must be provided free of charge, count as working time, and, where possible, take place during working hours.

Organisation of Working Time Act 1997, as amended

→ **Section 11**
Employees must have at least 11 consecutive hours' rest in every 24-hour period

→ **Section 12**
Employees cannot be required to work more than 4.5 hours without a 15-minute break, or 6 hours without a 30-minute break

→ **Section 13**
Employees must have at least 24 consecutive hours' rest each week; Sunday should generally be the weekly rest day

→ **Section 15**
Employees must not work more than an average of 48 hours per week, calculated over a reference period

→ **Section 17**
Employers must give at least 24 hours' notice of normal working hours or additional hours where schedules are not fixed

In Ireland, working time is regulated by the Organisation of Working Time Act 1997, which implements the EU Working Time Directive 2003/88/EC. Under this legislation, workers are entitled to a minimum of 11 consecutive hours of rest in each 24-hour period, one full day off per week, and a maximum average working week of 48 hours. Employers must maintain working time records for three years and make them available to the Workplace Relations Commission upon request.

These rules apply to all employees, including remote workers. Importantly, "working time" includes time spent answering emails, taking calls, or performing any duties at the employer's request, even if done outside of normal hours or remotely. As a result, activities such as responding to late-night emails may interrupt the statutory daily rest period.

To address growing concerns about the "always-on" work culture, the Workplace Relations Commission introduced a Code of Practice on the Right to Disconnect during the COVID-19 pandemic, which has been promulgated by statutory instrument (SI No. 159/2021). While not legally binding, it may be used to interpret the relevant provisions of the 1997 Act. The Code requires employers to create a *'Right to Disconnect Policy'* in consultation with employees or their representatives. This policy should make clear that staff are expected to disengage from work emails, messages, and calls outside their normal working hours and while on annual leave. However, it also recognises that occasional legitimate exceptions may arise, such as contacting staff to cover a shift at short notice, respond to emergencies, or meet business needs that demand contact outside of regular hours. Some roles may inherently involve out-of-hours working, depending on the nature of the service, the employee's responsibilities, or global time zone considerations, and this should be addressed in employment terms. The Code also highlights the challenges posed by flexible working arrangements, particularly when different employees follow conflicting schedules and stresses the importance of communication tone, advising employees to avoid creating a false sense of urgency in their messages that could pressure others to respond outside working hours. The Code further recommends that employers provide appropriate training for managers and establish clear procedures for resolving concerns. It outlines a tiered approach to complaints, starting with informal conversations and escalating to HR if needed.

The Employees (Provision of Information and Consultation) Act 2006, as amended

- → **Section 6**
  Requires employers to arrange the election or appointment of employees' representatives for information and consultation
- → **Section 7**
  Employers must enter negotiations to establish information and consultation structures when requested by at least 10% of employees (with minimum and maximum thresholds), or may do so voluntarily
- → **Section 8**
  Provides rules for creating a negotiated information and consultation agreement

The aim of the Act, which gives effect to EU Directive 2002/14/EC, is to establish a general framework that sets out minimum standards for employees' rights to information and consultation in any undertakings with at least 50 employees, whether public or private. It grants employees a general right to receive information and be consulted by their employer on issues that directly affect them. While the European Union (Transparent and Predictable Working Conditions) Regulations 2022 (discussed above) focuses on *individual* rights, this legislation focuses on employee's *collective* rights to information and consultation.

The 2006 Act, while not focused on digitalisation, provides a collective mechanism for employees to be informed and consulted, which could now include consultations about digitalisation, algorithmic management, monitoring technologies, AI in public procurement or other technological change affecting jobs. Under Section 3 of the 2006 Act, employers must inform and consult employees, through elected representatives, on: *"Decisions likely to lead to substantial changes in work organisation or in contractual relations."* Digitalisation for example, the introduction of AI systems, digital performance monitoring, automation or the design of employer's policy on the right to disconnect would, therefore, fall within this scope.

However, the right to information and consultation does not apply automatically. To start the process, at least 10% of employees in the organisation must make a request, with a minimum of 15 and a maximum of 100 employees. This request can be made directly to the employer or to the Labour Court (or its nominee). If the request goes to the Labour Court, it will inform the employer, check the details to confirm the number and names of employees involved, and then decide whether the request meets the required threshold. An employer can also decide to set up an information and consultation arrangement out of their own initiative.

European Union (Award of Public Authority Contracts) Regulations 2016 and additional legislation

→ **Regulation 18**
Sets out the principles of procurement: equality, non-discrimination, transparency and proportionality; prohibits designing procurements to exclude the rules or narrow competition; public contracts must require compliance with environmental, social and labour law

→ **Regulation 31**
Provides a special procedure for developing and purchasing innovative products, services or works

The European Union (Award of Public Authority Contracts) Regulations 2016 (S.I. No. 284 of 2016) is a statutory instrument that transposes the EU Public Procurement Directive 2014/24/EU into Irish national law. It establishes the legal framework governing how public authorities in Ireland must award contracts for goods, services, and works that exceed specified financial thresholds, in a transparent and non-discriminatory manner. It is supplemented by additional legislation, such as the European Union (Electronic Invoicing in Public Procurement) Regulations 2019 and sector-specific legislation relevant in the field of electronic communications which is exempt from the general public procurement rules. These include the European Union (Electronic Communications Code) Regulations 2022, as amended, and the Communications Regulation and Digital Hub Development Agency (Amendment) Act 2023.

Interestingly, Regulation 31 of the 2016 instrument sets out a special public procurement process that allows an Irish public body to work with one or more businesses to develop an innovative product, service, or works. However, the Regulations do not apply to the provision or exploitation of public communication networks or electronic communications services.

Public procurement is currently undergoing a digital transformation with many forms of e-procurement available.

Moreover, as AI systems are being increasingly used in public tenders, the adoption of the EU AI Act in 2024 has a significant impact on public procurement, both for public authorities conducting tenders and private companies participating in public procurement. In preparation for a public tender, authorities should carry out comprehensive risk assessments. Tender documentation should include detailed evaluation criteria that reflect the applicable legal, ethical, and technical standards. After the contract has been awarded, authorities must continue to monitor and audit AI systems to verify ongoing compliance with contractual obligations and to evaluate their performance over time. It is also crucial that staff responsible for overseeing AI systems receive appropriate training to ensure effective supervision and the ethical and accountable deployment of AI tools within public administration.

When a private company is providing a public service following a successful tender, and if it is deploying high-risk AI in employment matters (e.g. for recruitment, employee monitoring etc), it is then obliged, under Article 27 of the AI Act, to carry out a Fundamental Rights Impact Assessment to identify specific risks the system could pose to the affected individuals or groups, contingency plans and human oversight measures. Other employers in the private sector do not have this obligation.

Protected Disclosures Act 2014, as amended

→ **Section 5**
Defines a protected disclosure

→ **Section 12**
Prohibits penalisation (or threats of it) for making a protected disclosure

→ **Section 14A**
Creates offences for obstructing reporting, retaliating, breaching confidentiality, bringing vexatious proceedings etc

→ **Section 16**
Prohibits disclosure of the whistleblower's identity without explicit consent

→ **Section 23**
Nullifies any employment contract clause that seeks to prevent workers from making protected disclosures

The Protected Disclosures Act 2014 was primarily designed to protect workers who disclose information about wrongdoing in their workplace. In 2022, the Irish legislation was amended to implement EU's 'Whistleblowing' Directive 2019/1937. The Act protects workers who disclose information about "relevant wrongdoings" such as breaches of law, gross mismanagement, or endangerment of health and safety. These categories are broad enough to encompass digital-era issues such as unlawful data processing, intrusive employee surveillance, algorithmic discrimination, and unsafe use of automated systems.

Sections 11–13 of the 2014 Act provide strong safeguards against dismissal, penalisation, or other detriment for having made a protected disclosure, while Section 16 protects the identity of whistleblowers, except where disclosure is necessary for investigation or public safety. Importantly, Section 23 of the Act nullifies any employment contract clause that seeks to prevent workers from making protected disclosures.

The 2022 amendment has embedded many of the digitalisation aspects within the remit of the whistleblowing protection. Thus, Section 3 of the Act has been amended to explicitly include breaches in the protection of privacy and personal data, and security of network and information systems, as well as other areas impacted by AI, such as public procurement, financial services and product safety. This means that misuse of employee data, excessive or unlawful algorithmic monitoring, or security breaches of workplace systems can more clearly be cast as reportable.

Moreover, Section 3 of the Act has been revised to broaden the personal scope of protection, i.e. who can avail of whistleblowing protection. The definition of a "worker" has been expanded beyond typical employees to include also shareholders, volunteers, interns/trainees, non-executive directors, job applicants (insofar as they acquire information during recruitment), and more.

The 2022 amendment has also introduced new offences and penalties to deter companies from discouraging disclosures, threatening penalisation, or breaching confidentiality. As per a newly added Section 14A of the Act, the fines and penalties are substantial: up to €250,000, or imprisonment for up to two years (or both) in more serious cases.

The revised Act also establishes robust procedures for confidential and secure reporting, requiring public bodies – and, from 2023, many private organisations – to set up internal whistleblowing channels, designate impartial officers, and maintain confidentiality throughout the process. These institutional safeguards help ensure that disclosures about digital systems are handled responsibly, with oversight by the new Protected Disclosures Commissioner.

EU Platform Workers Directive 2024/2831

- → **Art. 2**
  Defines digital labour platform, platform work, platform worker
- → **Art. 4**
  Requires Member States to have procedures to verify correct employment status
- → **Art. 5**
  Introduces a rebuttable presumption that a person performing platform work has an employment relationship
- → **Art. 7**
  Bans certain data uses by automated systems (e.g. emotion/psychological state, private conversations, off-duty data)
- → **Art. 8**
  Platforms must carry out DPIAs, seek views of persons performing platform work and their representatives
- → **Art. 9**
  Platforms must inform workers, their representatives and authorities about automated monitoring/decision systems
- → **Art. 10**
  Requires regular human oversight and evaluation of automated systems' impact on working conditions and equal treatment, with involvement of workers' reps
- → **Art. 11**
  Gives workers the right to explanations and human contact for decisions taken or supported by automated systems, and to request a review
- → **Art. 12**
  Requires platforms to assess and control safety and health risks from automated systems and consult workers/representatives
- → **Art. 13**
  Extends existing EU information and consultation rights so that workers' representatives must be informed and consulted
- → **Art. 14**
  Where no workers' representatives exist, platforms must directly provide affected platform workers with written, clear and accessible information

In 2024, the European Union passed a Directive relevant to platform workers in the so-called 'gig economy'. It addresses two key challenges: misclassification of the worker status and algorithmic management. The Directive will be applicable in Ireland, but only once additional legislation is implemented on the national level. The deadline for enacting this implementing legislation for all the EU Member States including Ireland is December 2026. Therefore, while the rules outlined below are not yet effective, it is helpful to summarise them for workers to be aware of what changes are coming down the line.

The Platform Workers Directive will apply to individuals carrying out work for what is called "digital labour platforms". In practice, this definition often covers companies in the gig economy, such as food delivery apps or ride-hailing platforms including Uber, Deliveroo or others such as Upwork. However, any employer that uses digital systems to organise and monitor paid work, e.g. nursing agencies (even if it is just part of their business) should assess whether they fall within the scope of the Directive.

Article 5(1) of the Directive requires the EU countries to introduce a legal presumption that platform workers are employees unless the platform can prove otherwise. In the Irish context, there has already been some clarification regarding the employee test. In the aftermath of the Supreme Court's judgment in case The Revenue Commissioners v Karshan (Midlands) Limited t/a Domino's Pizza, the Revenue issued Guidelines for Determining Employment Status for Taxation Purposes followed by the government's Code of Practice on Determining Employment Status.

In terms of algorithmic management, the Directive is very significant as its Article 7(1) bans specific types of data processing which may otherwise be allowed by Article 9(2) GDPR. These include emotional/psychological data, private conversations (including with unions), data predicting trade union activity, biometric data and any surveillance outside of working hours. Furthermore, Article 10(5) of the Directive requires human oversight of major decisions, such as termination or suspension of accounts or of the employment relationship. In addition, the Directive also strengthens transparency obligations, as under Article 9 digital labour platforms must provide information on the use of automated monitoring and decision-making practices, including in recruitment and selection procedures. Overall, the Platform Workers Directive introduces a certain imbalance by granting these additional rights only to those individuals working for digital labour platforms and not to all employees.

FSU-Bank of Ireland Agreement

In 2025, the Irish Financial Services Union (FSU) concluded an AI agreement with Bank of Ireland. The agreement applies to all Band 1–3 employees of the Bank covered by collective bargaining agreements. It is aligned with the European Social Partners' declaration on the digitalisation of the financial sector and provides a framework for responsible AI use.

The agreement stresses some of the protections that already apply to all employees in Ireland based on some of the above listed legislation, such as that the use of AI in surveillance to monitor employees should be limited, transparent, proportional and in compliance with existing collective agreements and laws. Thus, any use of AI for monitoring or surveillance must be transparent, proportionate, and consistent with the employee's legal and contractual protections. The Bank must comply with GDPR, the EU AI Act, and national laws on data processing, meaning that employees have the right to know when and how AI systems collect or analyse data about them, and that such systems cannot be used intrusively or unfairly. Moreover, in line with the principle of human oversight, the agreement explicitly prevents the Bank from relying solely on automated systems to make decisions that have legal or significant consequences for staff, such as those involving performance, discipline, or changes to terms of employment.

To implement the AI Act's obligations regarding AI literacy, the Bank undertakes to provide relevant training during working hours so that employees can learn to use AI tools effectively and adapt to changing roles. This training commitment is tied to a broader right to employability: workers must be supported through reskilling or upskilling if AI changes the nature of their jobs.

The agreement frames this as a joint responsibility between the Bank and the FSU to help staff remain capable and secure in a more digital workplace. In this vein, the agreement confirms that existing job-security and change-management provisions remain in place and must be updated, not undermined, by the introduction of AI. If a role is transformed or replaced due to technological change, employees have the right to be considered for redeployment or retraining rather than redundancy.

The FSU-Bank of Ireland agreement was concluded in the aftermath of the aforementioned report on the employee experiences of technological surveillance in the Irish financial sector which recommended that employee surveillance issues could be addressed through collective bargaining. In 2025, the FSU was reported to be seeking a formal agreement on the use of AI with another major bank, AIB.

4. 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.

Checklist 1

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

Has management informed and consulted workers or their representatives about the planned introduction of the technology and its potential effects on work organisation?	→ Employees (Provision of Information and Consultation) Act 2006, s. 3; EU Platform Workers Directive Art. 13, GDPR Arts. 12–14
Has management carried out a Data Protection Impact Assessment (DPIA) for the proposed technology?	→ GDPR Art. 35
Were workers or their representatives consulted as part of the DPIA process?	→ GDPR Art. 35(9); Employees (Provision of Information and Consultation) Act 2006
Has management conducted an Occupational Health and Safety risk assessment prior to introducing the technology?	→ Safety, Health and Welfare at Work Act 2005 s. 19
Has management ensured qualified oversight, record-keeping, and a Fundamental Rights Impact Assessment of high-risk systems?	→ EU AI Act Arts. 27 & 29
Does the system involve any processing of special categories of personal data (e.g. biometric, emotional, or psychological data)?	→ GDPR Art. 9; EU AI Act Art. 5(1); Platform Workers Directive Art. 7
Has management ensured that workers' private communications, union activities, or off-duty data will not be monitored?	→ Platform Workers Directive Art. 7(1)(b)–(c); GDPR Art. 5(1)(b)
Are the purposes for data collection and processing clearly defined, limited, and communicated to employees in advance?	→ GDPR Art. 5(1)(b) (purpose limitation); GDPR Art. 13 (information duties
Have workers received clear, written information about how algorithms may affect scheduling, pay, or evaluation?	→ Terms of Employment (Information) Act 1994 as amended s. 3
Has management discussed how employees will be trained or supported to use and operationalise the technology safely and effectively?	→ EU AI Act Art. 4 (AI literacy); Terms of Employment (Information) Act 1994 as amended s 6G
Has management informed workers that their online or digital activity (such as email, browsing, login, or keystroke data) will be monitored?	→ GDPR Art. 5(1)(a) (transparency), Art. 13 (information duties); Safety, Health and Welfare at Work (General Application) Regulations 2007, Sch. 4, Art. 3(ii)
Has management explained whether automated tools or AI systems will be used to make or influence employment-related decisions (e.g., performance ratings, promotions, or disciplinary measures)?	→ GDPR Art. 22; EU AI Act Art. 26(11)
Is there a right to appeal or request a human review of any decision made or assisted by an automated system?	→ GDPR Art. 22(3); Platform Workers Directive Art. 10(5)
Has management confirmed that monitoring systems will not operate outside working hours, or in private communications (including union activity)?	→ EU Platform Workers Directive Art. 7(1); Organisation of Working Time Act 1997; GDPR Art. 5(1)(a)

Checklist 2

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

Has any new functionality been added (for example, tracking time, performance scores, or location) that wasn't part of the original system?	→ GDPR Art. 5(1)(b); Safety, Health and Welfare at Work (General Application) Regulations 2007, Sch. 4, Art. 3(ii)
Has management informed workers about any changes in the purpose of data collection or processing?	→ GDPR Art. 13; Employees (Provision of Information and Consultation) Act 2006
If new uses of data have been introduced, has management carried out and shared an updated Data Protection Impact Assessment (DPIA)?	→ GDPR Art. 35(11)
Are there clear procedures for workers to see the data being used about them (e.g., productivity reports, attendance logs, or app-generated performance metrics?	→ GDPR Arts. 15–17 (rights of access, rectification, erasure)
Have any automated tools started making decisions (e.g. shift allocation, performance grading) without a human review?	→ GDPR Art. 22; EU AI Act Art. 14
When a worker disagrees with an automated decision, is there a human contact point to review it?	→ GDPR Art. 22(3); Platform Workers Directive Art. 10(5)
Are the monitoring or tracking systems being used outside of working hours or in private communications?	→ EU Platform Workers Directive Art. 7(1); Organisation of Working Time Act 1997; GDPR Arts. 5–6
Has the company reviewed whether the technology has caused new health or stress risks (e.g. constant alerts, increased pace, screen fatigue)?	→ Safety, Health and Welfare at Work Act 2005 s. 19
Has the company provided training when systems were updated, or new ones added?	→ EU AI Act Art. 4 (AI literacy); Terms of Employment (Information) Act 1994 as amended s 6G
Are whistleblowing channels available and trusted for reporting misuse of technology or unfair surveillance?	→ Protected Disclosures Act 2014 as amended s. 6A
If data from a digital system is used in disciplinary or performance-related discussions, can the worker and their representative see the data it was based on and the algorithm's interpretation or score?	→ GDPR Arts. 15–16

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.

A relevant bargaining topic for consultation prior to the deployment of a new digital technology could be:

→ Setting clear limits on the processing of workers' data. For example, information collected for security or operational purposes (such as swipe-card entries or GPS routes) cannot be used for performance evaluation or disciplinary measures.

→ Ensuring transparency. Workers' representatives must receive plain-language explanations of what data are collected, who accesses them, and for what purpose.

→ Participation rights. No new digital technologies can be introduced without prior social dialogue / collective bargaining.

If management introduces digital systems that monitor workers' activity (for instance, email, chat, or platform data), workers could bargain for:

→ Transparency of monitoring. That employees are informed in advance about what is being monitored, for how long, and how the information will be used.

→ Protection of private communications. That monitoring systems must exclude private or union-related correspondence and cannot record off-duty activity.

→ Proportionate use. That any monitoring be limited to what is strictly necessary to ensure network security or fulfil contractual duties.

If management plans to deploy an AI-based decision-making tool (for example, for shift allocation or performance scoring), workers could bargain for:

→ Human oversight. That all significant employment decisions be reviewed and approved by a qualified human manager.

→ Right to explanation and appeal. That workers have the right to understand how a decision was reached and to request a human review if they believe it is unfair or inaccurate.

→ Regular evaluation of bias. That systems be tested for discriminatory outcomes and corrected where bias is detected.

If management introduces a new HR or scheduling app that collects personal or location data, workers could bargain for:

→ Data limitation. That the app cannot collect information from phone sensors or GPS outside agreed working hours.

→ Right of access. That workers and their representatives can obtain copies of the raw data used in any disciplinary or performance process.

→ Voluntary use of personal devices. That no employee be compelled to install work-related apps on personal phones without consent and reimbursement of costs.

If management updates existing digital systems or introduces new ones, workers could bargain for:

→ Training rights. That all affected employees receive paid, practical training before the system becomes mandatory.

→ Representative training. That union or staff representatives be offered specialised training on digital rights and AI governance issues.

If management has carried out a data protection / health and safety risk / fundamental rights assessment (legally required or voluntary), workers could bargain for:

→ Participation rights. That worker representatives be formally involved in conducting and reviewing these assessments.

→ Access to full documentation. That they can see the entire assessment, not just a summary.

→ Follow-up consultation. That there be joint meetings to evaluate whether agreed remedies actually reduced the identified risks.

If digitalisation changes workloads or intensifies monitoring, workers could bargain for:

→ Regular reviews of workload, screen-time fatigue, and stress levels.

If management contracts external technology or cloud services, workers could bargain for:

→ Transparency about external services. That all external providers handling employee data be identified and disclosed.

→ Joint oversight to review the external service's performance and data handling practices.

If workers are expected to remain reachable or digitally connected outside normal hours, they could bargain for:

→ Enhanced right to disconnect. That no data or activity monitoring occur outside scheduled hours.

→ Technical safeguards. That systems automatically suspend monitoring when the employee is logged out.

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!

This guide offers an overview of how digital technologies, and particularly artificial intelligence, are transforming work in Ireland, while highlighting the accompanying legal, ethical, and industrial relations challenges. It outlines current practices such as the use of AI tools to assist in workflow management, digital scheduling in healthcare, and monitoring systems including GPS tracking, keystroke logging, and swipe-card data. These examples highlight both the opportunities and challenges that arise as digitalisation becomes embedded in everyday work.

A key observation is that technological change is progressing faster than awareness of the rights and obligations it brings. Many employees might be uncertain about how their data are processed or how automated systems influence decisions affecting them. The guide therefore emphasises the importance of transparency, consultation, and human oversight when new digital tools are introduced.

From a practical perspective, several existing legal frameworks already provide guidance for managing these developments responsibly. The GDPR and Data Protection Act 2018 set clear standards for fairness and transparency in handling personal data. The EU AI Act introduces new requirements for oversight and accountability in high-risk AI systems, while Irish employment, health and safety, and equality laws continue to apply in digital contexts. Together, these instruments establish a legal foundation that can support fair and compliant use of technology at work. The reflection also points to the growing role of European law in shaping national labour standards, from the Platform Workers Directive to evolving employment equality and transparency legislation.

Importantly, the report provides practical examples of how these laws can be turned into bargaining power. This report's "questions for workers" and "bargaining topics" sections are especially useful checklists for anyone preparing to engage with management about new technologies. These resources are designed to support dialogue, promote understanding of rights and responsibilities, and encourage balanced approaches to technology use in the workplace. The hope is that unions can use the report to open conversations about data use, workload, and AI transparency, turning rights on paper into everyday protections.

7.
Annex – Links to the Laws and Agreements Covered

→ **GDPR (General Data Protection Regulation (EU) 2016/679)**
PDF here: https://eur-lex.europa.eu/legal-content/EN/TXT/ PDF/?uri=CELEX:32016R0679

→ **Data Protection Act 2018**
PDF here: https://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/pdf

→ **The EU AI Act (Regulation (EU) 2024/1689)**
PDF here: https://eur-lex.europa.eu/legal-content/EN/TXT/ PDF/?uri=OJ:L_202401689

→ **Safety, Health and Welfare at Work Act 2005,** read together with the → **Safety, Health and Welfare at Work (General Application) Regulations 2007**
PDF of 2005 Act: https://www.irishstatutebook.ie/eli/2005/act/10/enacted/en/ PDF

→ **Employment Equality Acts 1998–2015, as amended**
PDF of 1998 version here: https://www.irishstatutebook.ie/eli/1998/act/21/enacted/en/html

Note: This Act was subsequently amended by later Acts (e.g., 2004, 2011-13). See consolidated/updated version here: https://revisedacts.lawreform.ie/eli/1998/act/21/revised/en/html

→ **Terms of Employment (Information) Act 1994**, as amended by the → **European Union (Transparent and Predictable Working Conditions) Regulations 2022**
PDF of EU Transparent and Predictable Working Conditions here: https://www.irishstatutebook.ie/eli/2022/si/686/made/en/ PDF

→ **Organisation of Working Time Act 1997**, as amended
PDF here: https://www.irishstatutebook.ie/eli/1997/act/20/enacted/en/ PDF

→ **The Employees (Provision of Information and Consultation) Act 2006**, as amended
PDF here: https://www.irishstatutebook.ie/eli/2006/act/9/enacted/en/ PDF

→ **European Union (Award of Public Authority Contracts) Regulations 2016**
PDF here: https://www.irishstatutebook.ie/eli/2016/si/284/made/en/pdf

→ **Protected Disclosures Act 2014**, as amended
PDF here: https://www.irishstatutebook.ie/eli/2014/act/14/enacted/en/ PDF

→ **EU Platform Workers Directive 2024/2831**
PDF here: https://eur-lex.europa.eu/legal-content/EN/TXT/ PDF/?uri=CELEX:32024L2831&utm_source=-chatgpt.com

→ **FSU-Bank of Ireland Agreement**
PDF here: https://www.fsunion.org/assets/files/pdf/boi_fsu_ai_agreement.pdf

8.
Glossary List

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

A

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

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

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

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

B

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

C

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

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

D

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

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

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

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

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

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

Digital technologies Digital technologies are electronic tools, devices, software, and data-processing applications that create, collect, store, transmit, or analyse digital data. In workplaces, this includes items such as computers, mobile devices, biometric scanners, cameras, GPS devices, software applications, platforms, and databases.

These technologies generate and process data that can be used in organising, monitoring, or managing work. Digital technologies are the individual electronic tools and applications.

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

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

E

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

F

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

H

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

I

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

O

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

P

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

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

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

R

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

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

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

S

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

W

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

About the author

Marta Lasek-Markey, Assistant Lecturer in Law,
Technological University of Dublin

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