

*A report for the Trades Union Congress
by the AI Law Consultancy*



Technology Managing People – the legal implications

Robin Allen QC and Dee Masters
Cloisters

cloisters.com
ai-lawhub.com



Contents

| | |
|--|----|
| Executive summary | 6 |
| Introduction | 9 |
| Chapter 1 – Setting the scene: the new technologies and their impact on employment..... | 14 |
| Summary | 14 |
| Understanding the new technologies and their effects | 15 |
| <i>Artificial Intelligence</i> | 15 |
| <i>Algorithms</i> | 16 |
| <i>Machine learning</i> | 17 |
| <i>Automated decision making</i> | 18 |
| <i>Profiling</i> | 19 |
| The impact of Covid-19 | 20 |
| <i>The range of effects</i> | 20 |
| <i>Fear and trust</i> | 21 |
| <i>The “always-on” culture</i> | 23 |
| <i>Concerned bodies</i> | 24 |
| The UK’s Labour Law code and related provisions | 26 |
| <i>The Common law</i> | 27 |
| Mutuality..... | 27 |
| Personal service | 27 |
| Trust and confidence | 28 |
| The implications of trust and confidence between employer and employee..... | 30 |
| <i>The legislative framework</i> | 31 |
| Statutory rights to fair process | 31 |
| Health and safety | 32 |
| Equality | 32 |
| Data protection and privacy rights | 32 |
| Privacy | 33 |
| Collective rights and obligations | 33 |
| <i>The special status of workers</i> | 34 |
| “Red line” limits to the use of AI and ADM in the workplace | 34 |
| Chapter 2 – The capacity of UK laws to control the use of AI systems in the workplace..... | 38 |
| Summary | 38 |

| | |
|--|-----------|
| A: Right to work without discrimination | 42 |
| <i>How bias can occur in AI systems</i> | 43 |
| <i>The implications of biased AI systems</i> | 44 |
| <i>The Equality Act 2010</i> | 45 |
| <i>Case Study A: Online job advertising marginalising female candidates</i> | 47 |
| <i>The problem of getting to know what has happened</i> | 49 |
| <i>Case Study B: The impact of biometric data analysis to score applicants</i> | 50 |
| <i>General conclusions about the Equality Act 2010</i> | 52 |
| B: Principles of observability and transparency | 54 |
| <i>"The black box"</i> | 54 |
| <i>Using the UK GDPR to find out what happened</i> | 56 |
| <i>Opening the "black box" through litigation</i> | 60 |
| <i>Conclusion about the UK GDPR</i> | 61 |
| <i>International trade in intellectual property rights</i> | 61 |
| <i>Conclusion about trade in IPRs</i> | 65 |
| C: Right to privacy | 66 |
| <i>Case Study C: Monitoring productivity</i> | 66 |
| <i>Conclusion about the right to privacy</i> | 69 |
| D: Right to data protection | 70 |
| <i>Conclusions about data protection</i> | 71 |
| E: Protection from AI-powered decisions that are irrational or unfair | 75 |
| <i>Case Study D: The impact of flawed algorithms on workers and employees</i> | 75 |
| <i>Conclusions about the protections from irrational and unfair decisions</i> | 76 |
| F: Management within a personal relationship | 78 |
| <i>Conclusion about management within a personal relationship</i> | 79 |
| G: Protection of workers' private time from the intrusion of technology | 80 |
| H: Rights of association and bargaining | 83 |
| Chapter 3 – Recommendations for action and reform | 87 |
| Summary | 87 |
| The present opportunity to shape the legal landscape | 87 |
| Promoting the case for better regulating AI and ADM in the workplace | 90 |
| Guiding principles that should shape regulatory reform | 93 |
| <i>"Red line" limits should not be negotiable</i> | 93 |
| <i>"High risk" applications must be regulated</i> | 93 |

| | |
|--|------------|
| <i>Regulation must be targeted</i> | <i>94</i> |
| <i>Enhanced rights to data reciprocity must be established</i> | <i>95</i> |
| <i>Regulation must be proportionate, practical, certain, and workable for all</i> | <i>95</i> |
| <i>A pre-emptive approach to governance should be established</i> | <i>97</i> |
| <i>New initiatives should be established collectively</i> | <i>97</i> |
| General recommendations for legislation | 97 |
| <i>1: The amendment of UK data protection legislation to enact a universal right to explainability in relation to “high risk” AI or ADM systems in the workplace with a right to ask for a personalised explanation along with a readily accessible means of understanding when these systems will be used.</i> | <i>97</i> |
| Meaningful information | 98 |
| Section 1 particulars | 98 |
| AI registers | 98 |
| <i>2: The Employment Rights Act 1996 should be amended to create a right, which can be enforced in the Employment Tribunal, for workers not to be subject to detrimental treatment, including dismissal, due to the processing of inaccurate data.</i> | <i>99</i> |
| A right not to suffer detriment from inaccurate data or other breach of data regulation | 99 |
| <i>3: The UK’s data protection regime should be amended to state that discriminatory data processing is always unlawful.</i> | <i>100</i> |
| <i>4: The burden of proof in relation to discrimination claims which challenge “high risk” AI or ADM systems in the workplace should be expressly reversed.</i> | <i>101</i> |
| <i>5: Provision should be made to ensure that all actors in the “value chain” leading to the implementation of AI and ADM in the workplace are liable for discrimination subject to a reasonable step defence</i> | <i>101</i> |
| <i>6: No international trade agreement should protect intellectual property rights from transparency in such a way as to undermine the protection of employees and workers’ rights.</i> | <i>102</i> |
| <i>7: Equality Impact Audits in the workplace should be made mandatory as part of the Data Protection Impact Assessment process and made readily accessible to workers, employees, and their representatives.</i> | <i>103</i> |
| <i>8: Provision should be made for joint statutory guidance on the steps that should be taken to avoid discrimination in consequence of these new technologies.</i> | <i>104</i> |
| <i>9: There should be statutory guidance for employers on the interplay between AI and ADM in relation to Article 8 and key data protection concepts in the UK GDPR.</i> | <i>104</i> |
| <i>10: There should be a statutory right for employees and workers to disconnect from work so as to create “communication free” time in their lives.</i> | <i>106</i> |
| <i>11: There should be a comprehensive and universal right to human review of decisions made in the workplace that are “high risk”.</i> | <i>106</i> |

| | |
|---|------------|
| <i>12: There should be an express statutory right to personal analogue engagement – an “in person engagement” – in relation to decisions made in the workplace which are “high risk” such as may have any significant impact on the working life of employees and workers.....</i> | <i>107</i> |
| Recommendations concerning a bipartisan approach to data rights..... | 108 |
| <i>13: Employees and workers should have a positive right to “data reciprocity”, to collect and combine workplace data so as to better understand the ways in which new technologies are being and can be used in the workplace, and to take advantage of this information for themselves.</i> | <i>108</i> |
| <i>14: Trade unions should have a formal data-gathering role in relation to member data so that they can effectively monitor the use of “high risk” AI and ADM in the workplace.</i> | <i>109</i> |
| <i>15: Trade unions should seek recognition as data subject representatives under the UK GDPR.</i> | <i>110</i> |
| Recommendations concerning collective bargaining and a multi-stakeholder approach | 112 |
| <i>16: There should be a statutory duty to consult trade unions in relation to the deployment of “high risk” AI and ADM systems in the workplace directly or through a third party.....</i> | <i>112</i> |
| <i>17: Employment-focused ethical principles in relation to “high risk” AI and ADM systems should be established.</i> | <i>112</i> |
| About the authors..... | 114 |

Executive summary

We present our Report to the Trades Union Congress (TUC) on the legal implications of Artificial Intelligence (AI) systems in the post-pandemic workplace.

Our Report must be read in conjunction with the TUC's own paper published in the Autumn of 2020 called "*Technology managing people: The Worker Experience*" (the "*Worker Experience Report*"), published on 30 November 2020, which provides an invaluable and unique insight into the way in which AI is already being used and perceived in the workplace.¹

The TUC has an overarching purpose, which is "to make the working world a better place for everyone"² – an aim we can all share. We believe that AI systems have much to contribute and should be embraced, yet these new technologies need to be deployed in the *right* way. Our Report concludes that there are real problems with the deployment of AI in the *wrong* way and explains that these difficulties must be addressed by an effective legal system.

In some respects, our concerns can be met by the effective use of existing law. In others, our analysis shows that there are significant gaps in the legal protection, and we conclude that, even where current laws are potentially effective, there are important steps that should be taken to ensure that these laws are better known and more effective.

In the [Introduction](#), we set out why the work by the TUC is so timely and so important, noting the consequences for society if we do not reflect on the implications for the uncontrolled development and use of AI systems in the workplace.

¹ See https://www.tuc.org.uk/sites/default/files/2020-11/Technology_Managing_People_Report_2020_AW_Optimised.pdf

² See [here](#).

In [Chapter 1](#) we then set the scene for our analysis, explaining how new technologies involving AI systems are impacting on the modern employment relationship. This Chapter outlines the nature of these new technologies and highlights the trust deficit that has arisen. It describes key aspects of the legal relationship between the employer and those who work in its enterprise and points out that there are gaps in legal protections for employees and workers.

It concludes by setting out "*red lines*" that should not be crossed if AI systems are to exist in harmony with, rather than undermine, the basis for the modern employment relationship. We urge the TUC to adopt these *red lines* as the basis for its future work in this field.

[Chapter 2](#) continues this theme by discussing the capacity of UK laws to control the use of AI systems in the workplace, explaining how bias can occur when these systems are used and discussing more widely what are the implications of using them by reference to four case studies. This Chapter also contains 15 specific conclusions about the legal consequences of using AI systems in the workplace.

In our final [Chapter 3](#), we explain the principles that we believe should shape the future regulation of AI systems used in the workplace with 17 recommendations for action and reform. These are directed to legislators, regulators, and to the trade union movement. We believe that they will be welcomed too by any business wishing to adopt a modern and human-centric approach to AI.

This is our Report, but we must state clearly that it would not have been possible to undertake this work without the great support we have had from the members of the TUC's AI working group, in particular Mary Towers, Policy Officer (TUC), Andrew Pakes, Director of Communications and Research (Prospect), Alison Roche (UNISON), Jenny Lennox, Bargaining and Negotiations Official (UCU), Steve Garelick (GMB) and support from our colleagues within [Cloisters barristers' chambers](#), especially Joshua Jackson and Tamar Burton.

Working together as the AI Law Consultancy, we have looked at these kinds of problems for several years now, engaging with them from many different angles. We

are therefore delighted to have been asked to help facilitate the TUC's engagement with the legal implications of new technology in the workplace.

It will be seen from the detail of our Report that there is much to be done. We very much hope that our Report will help the TUC to plan an appropriate course of action.

It has been a privilege to work with the TUC on this important issue.

Robin Allen QC Dee Masters

**The AI Law Consultancy
Cloisters**

11 February 2021

Introduction

In January 2016, Klaus Schwab, the Founder and Executive Chairman of the World Economic Forum, declared that the world was entering the “*Fourth Industrial Revolution*”, saying:³

We stand on the brink of a technological revolution that will fundamentally alter the way we live, work, and relate to one another. In its scale, scope, and complexity, the transformation will be unlike anything humankind has experienced before.

He was talking about the impact of the accelerating increase in computing power and was seeking to alert the world to its capacity to analyse and use data to make and execute decisions about and for us. His concern was the effect that this could have on every aspect of our lives if it were to be uncontrolled. His aim was to highlight the absolute necessity that humans should be *in charge* of this process and not merely victims, arguing that:

...the response to it must be integrated and comprehensive, involving all stakeholders of the global polity, from the public and private sectors to academia and civil society.

He concluded with a warning:

³ “[The Fourth Industrial Revolution: what it means, how to respond](#)” World Economic Forum, 14 June 2016.

In the end, it all comes down to people and values. We need to shape a future that works for all of us by putting people first and empowering them. In its most pessimistic, dehumanized form, the Fourth Industrial Revolution may indeed have the potential to “robotize” humanity and thus to deprive us of our heart and soul. But as a complement to the best parts of human nature – creativity, empathy, stewardship – it can also lift humanity into a new collective and moral consciousness based on a shared sense of destiny. It is incumbent on us all to make sure the latter prevails.

His warning was apt then; it is even more so now. Less than five years from the publication of Schwab’s book, it is certain that the Fourth Industrial Revolution is truly upon us. By September 2020, across the EU27, Norway, Iceland, and the UK, over 40% of enterprises have adopted at least one AI-powered technology and a quarter have adopted at least two, while a further 18% have plans to adopt AI in the next two years.⁴ Similar or even greater statistics can be produced for other parts of the developed world.

Has Klaus Schwab’s warning been heeded?

Since his warning, there has been much talk about the challenges posed by new technologies, with academic scholars, engineers, philosophers, and others discussing the ethics of using Artificial Intelligence and similar technologies. There is also a growing realisation within some bodies that advise the UK government that specific regulation is needed. Yet the fact remains that *no* new legislation has been passed in the UK to amend and improve labour and trade union laws to make them fit to meet the Fourth Industrial Revolution.⁵ So it is greatly to its credit that the TUC, having unparalleled access to the lives of workers, has decided to take a lead and make proposals as to how workers, employees and job applicants should be protected.

Recognising its almost unique capacity to gain a wide perspective on the effects that these new technologies are already having, the TUC committed in 2019 to being at the

⁴ See “*European enterprise survey on the use of technologies based on artificial intelligence*”, the final Report of a study prepared for the European Commission DG Communications Networks, Content & Technology, prepared by Ipsos Belgium and the International Centre for Innovation Technology and Education, at the Solvay Brussels School of Economics & Management, at the Université Libre de Bruxelles, 2020, European Union.

⁵ That is not to say that there has been no discussion of the need for new legislation.

forefront of the debate about what needed to be done. It resolved that the risk of dehumanisation through the inappropriate use of these systems must be addressed fully, while also recognising the undoubted potential for new technologies used appropriately to have positive effects for all in the workplace. Above all, it resolved that new technologies should not cause a loss of transparency and accountability, nor a loss of human interaction leading to an increase in alienation.⁶

The TUC's determination to shape the debate concerning technology in the workplace is especially timely in view of the lockdowns imposed to address the Covid-19 pandemic, first in March 2020 and later in autumn and winter of 2020/1. It is widely acknowledged, including by the Council of Europe's Ad Hoc Committee on Artificial Intelligence known as CAHAI,⁷ that the lockdowns have accelerated radical change to the use of these new technologies both generally and in the work environment.

The TUC's starting point has been to get at the facts by surveying unions, employees, and workers to find out what is happening in the workplace right now.

Over the summer of 2020,⁸ the TUC launched the first-ever survey of the ways in which UK employers were deploying AI and automated decision-making (ADM) to recruit, monitor, manage, reward, and discipline their workforce.⁹ The conclusions of the survey are set out in the *Worker Experience Report*.

The *Worker Experience Report* measured the impact of AI technologies on employees and workers in the UK. It has shown not just how much these new technologies are being used in the workplace but, very importantly, how little the implications of this are understood by those workers and employees, and in many cases by the employers who use such products, who often have purchased them from third parties with little understanding of their implications.

⁶ See TUC Congress Motion "[Composite 06 Collective voice and new technology](#)" 2019.

⁷ See "TOWARDS REGULATION OF AI SYSTEMS: Global perspectives on the development of a legal framework on Artificial Intelligence (AI) systems based on the Council of Europe's standards on human rights, democracy and the rule of law", CAHAI, December 2020.

⁸ The authors are grateful to the TUC for sharing with them the approach it proposed to take in conducting this survey at a very early stage.

⁹ Whilst there was some international data which indicated that AI was growing in the workplace (for example, a 2018 [US source](#) suggested that 55% of human resource managers were intending to use AI over the following 5 years), there was no meaningful analysis of the precise ways in which these types of technology were being used in the UK prior to the TUC's survey.

In particular, the *Worker Experience Report* has highlighted how frequently the introduction of these new technologies has not been subject to any real consultation. It underlines just why those fears, aptly expressed by Klaus Schwab, must be taken seriously and that the time to act is *now* if these new technologies are not to be allowed to reduce personal autonomy in the workplace to vanishing point.

To achieve this, it is becoming clear not only that existing laws must be used to the full but that there is a need for further context-specific regulation to be identified and enacted. In other words, having described what is happening in the *Worker Experience Report*, the next step is to consider *how* the TUC (and in due course the leaders of this country) should act on this information.

It is not difficult to summarise the tasks ahead. First the TUC must identify the principles by which the use of AI and ADM in the workplace should be judged. Next the capacity of the UK's Labour Law code, and its Data Protection and Human Rights laws, to address and forestall the problems that are emerging must be analysed. Through this legal gap analysis, we can gain an understanding of *how* and *where* regulations need to be amended or enacted to make them fit for the Fourth Industrial Revolution.

This is a moment to be reminded of the campaigning slogan of the disability movement in the 1990s: "*Nothing about us without us*". That slogan demanded that all and any policies that impacted on disabled persons should never be determined without their participation.¹⁰ This slogan has a contemporary resonance because the *Worker Experience Report* shows how AI technologies are increasingly being used in the employment sphere without the knowledge, understanding or participation of workers, employees, and trade unions.

The *Worker Experience Report* and our research for this Report have made us certain that this Fourth Industrial Revolution must be one that truly works for us all, and that cannot be allowed to bring in an era in which "*Almost everything about us is happening without us*".

In short, this Report shows that this is now the time to take steps to ensure that these technologies are used in the workplace only when, and where, they are understood, and that those affected by them have a say in their use. We hope that the analysis and

¹⁰ This proposition has continued as non-negotiable ethic for the community of persons with disabilities through every stage of adopting the [UN's Convention on the Rights of Persons with Disabilities](#) 2006, and beyond.

recommendations in our Report, if adopted, can help ensure that Klaus Schwab's worst fears are avoided in the UK.

Chapter 1 – Setting the scene: the new technologies and their impact on employment

Summary

In [Chapter 3](#), the final chapter of this Report, we shall both set out a series of steps that we recommend the trade union movement takes to address the problems arising from the Fourth Industrial Revolution and make proposals for legislative changes. These are the end-product of a legal analysis conducted in light of the TUC's *Worker Experience Report* and our own knowledge and experience gained in addressing AI issues. To explain how we have reached these conclusions, we will need to address a central question: How far can current laws control the inappropriate use of AI systems in the workplace? That is the focus of [Chapter 2](#).

But first in this Chapter, we need to set the scene for this analysis. We need to explain how new technologies, involving AI systems, are impacting on the modern employment relationship.¹¹

To do this we must start by summarising the nature of the new technologies that are currently known to be deployed in the workplace, noting some of the specific effects of Covid-19 in accelerating the use of new technology. Among these we shall note how there is little trust that these technologies are being used fairly, ethically, legally, and without discrimination.

Next, we outline key aspects of the legal relationship between employer and employee and workers, which are being affected by these new technologies and which in turn play a role in determining what is and is not lawful. In this section we shall note how these new technologies have a capacity to undermine essential aspects of the modern employment relationship. We point out how this should not be acceptable, drawing clear “red lines” beyond which AI systems must not be used. We shall return to these “red lines” in [Chapter 3](#), when we discuss their implications further.

¹¹ Our Report is not limited to those who work with a contract of employment; we recognise that there are many workers in the gig economy and elsewhere that are not in business on their own account but have a personal and dependent relationship on a specific employer. Such workers are recognised to be in a special category by the UK's Labour Law code and have been given some of the protections of employees.

Understanding the new technologies and their effects

- 1.1. The TUC, and many among the wider public, already know that there are a range of new technologies that are being used in the workplace. These use AI, ADM, ML, and algorithms.¹²
- 1.2. To know this generally is one thing: to understand what is happening is quite another. While the way they work is complex, ignorance of the basic facts about these technologies is no longer an option if we are to heed Klaus Schwab's warning about the possible effects of the Fourth Industrial Revolution that we set out in our Introduction. So, what is involved?

Artificial Intelligence

- 1.3. We start with AI. There is no one, single, universally agreed definition of the concept of AI,¹³ although it is a notion that was first identified as early as the 1950s.¹⁴ We find it helpful, however, to think about AI as being "*the science of making machines smart*", a phrase coined by Professor Frederik Zuiderveen

¹² In this Report we shall distinguish between these processes when it is necessary to do so, but shall also refer to "AI systems" as indicating the general range of new technologies that the TUC must address.

¹³ [S. 23A\(4\) of the Enterprise Act 2002](#), defines "Artificial Intelligence" to mean "technology enabling the programming or training of a device or software to use or process external data (independent of any further input or programming) to carry out or undertake (with a view to achieving complex, specific tasks)—(a) automated data analysis or automated decision making; or (b) analogous processing and use of data or information." This is the only current UK statutory definition of the concept, and it is not directly relevant to the subject matter of this Report as it concerns regulation by the Competition and Markets Authority of certain business transactions. Nonetheless, it might be borne in mind, as the definition closely relates to the concept of AI with which this Report is concerned.

¹⁴ Many people credit Alan Turing (1912-1954), who worked on the Enigma machine during the Second World War, with the idea as a result of his paper [Computing Machinery and Intelligence](#), first published in 1950 in *Mind*, in which he famously said, "I propose to consider the question, 'Can machines think?'". See now, Turing, A.M., 2009. Computing machinery and intelligence. In *Parsing the Turing test* (pp. 23-65). Springer, Dordrecht.

Borgesius.¹⁵ At its core is the idea that machines might be made to work in the same way as humans, only faster, better, and more reliably.

1.4. In broad outline, there are five parts to creating AI systems:

- an understanding of human thought processes and how they proceed to action
- a logical analysis of such processes
- a means to describe that analysis as a set of instructions for a machine
- the supply of data to the machine on which it can then work, and then finally
- the construction of a machine that can do this work more quickly than a human.

1.5. Once created, the AI system will operate on fresh data supplied to it in any number of different ways, such as from sensors, records, scanners and so on. Armed with that information, AI systems draw conclusions that can then be acted on by humans or can cause other machines to take action without further human involvement. Each of these steps should be kept in mind during our discussion in this Report.

Algorithms

1.6. The instructions to the machine come from algorithms. These are the instructions to a computer to use a data input to create a specified output. In the early days of computing, they would sometimes be called computer programs, setting out the logical steps that the computer must follow in addressing the data presented to it.

¹⁵ Zuiderveen Borgesius, F., 2018. [Discrimination, artificial intelligence, and algorithmic decision-making](#).

Machine learning

- 1.7. Now computing power is so much greater, more can be done with these algorithms. The computing machine can be programmed to learn; this is ML. ML is one of the most significant features of AI systems. It is what makes “*the machines smart*” in that it allows the algorithms in the AI system to self-create and adapt by learning from correlations it can find in a data input (often known as the “training set”) to make predictions that relate to another data set.
- 1.8. The [International Association of Privacy Professionals](#) has neatly described ML in this way:

Machine learning is a technique that allows algorithms to extract correlations from data with minimal supervision. The goals of machine learning can be quite varied, but they often involve trying to maximize the accuracy of an algorithm’s prediction. In machine learning parlance, a particular algorithm is often called a “model,” and these models take data as input and output a particular prediction. For example, the input data could be a customer’s shopping history and the output could be products that customer is likely to buy in the future. The model makes accurate predictions by attempting to change its internal parameters — the various ways it combines the input data — to maximize its predictive accuracy. These models may have relatively few parameters, or they may have millions that interact in complex, unanticipated ways. As computing power has increased over the last few decades, data scientists have discovered new ways to quickly train these models. As a result, the number — and power — of complex models with thousands or millions of parameters has vastly increased. These types of models are becoming easier to use, even for non-data scientists, and as a result, they might be coming to an organization near you.

- 1.9. For many the idea that a machine can learn to make correlations in ways that it was not originally asked to do can seem fantastical. Yet it is a process that is now common and often, but by no means always, beneficial.

Automated decision making

- 1.10. ADM is by contrast a relatively straightforward concept. Strictly ADM occurs when decisions or conclusions are reached without any direct human involvement,¹⁶ for example, when a highway agency has a system that issues a speeding fine based on a camera's assessment of a car's speed.
- 1.11. In practice, there are AI systems that are sometimes described as ADM, even though they are not entirely automatic, because the degree of human involvement is very limited. For example, a human might undertake some formal task, such as handling a document but the human agency in the decision is minimal. Sometimes the human decision making is largely illusory, for instance where a human is ultimately involved only in some formal way in the decision what to do with the output from the machine. In those situations, the machine output is given such a dominant role in the decision-making that the human in practice accepts it uncritically as being determinative.
- 1.12. This can occur in various ways. One way is where frequent repetition or use of the AI system leads to a kind of mental disengagement. In this context the human no longer thinks it necessary to consider the output in a critical way. Yet it is important to be aware that frequent use is not the only basis for such uncritical engagement. There can also be a simple bias toward accepting the output from an AI system as always being "right". These two reasons can of course co-exist and often will do so. The key point is that they have the same effect: they lead to decisions that are effectively automated because they lack any real human agency.
- 1.13. Some AI and ADM is perfectly innocuous, useful, and low risk. For example, it is difficult to imagine that anyone will object to an app that uses AI and ML to predict the quickest route from A to B at a certain time of the day. Such systems are used daily by delivery drivers to minimise stress and maximise productivity and, provided drivers are not as a result overburdened, their

¹⁶ See the definition of the concept used by the Article 29 Data Protection Working Party in its "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01)" Section B. The Guidelines which are available [here](#), have been adopted by the European Data Protection Board at its first plenary meeting. See also Article 22 UK GDPR discussed in this Report [here](#).

working life is enhanced. Equally, an automated HR system that tracks training records of staff identifying “gaps”, or a diary tool that schedules meetings at a time when the greatest number of participants are available, will often be useful and helpful. However, there are other applications that must be more carefully analysed.

Profiling

- 1.14. One of the most potentially problematic forms of AI and ADM is “*profiling*”. The concern regarding profiling is so great that it is already subject to special rules under data protection legislation, thus it is defined under Article 4(4) of the [UK General Data Protection Regulation](#) (UK GDPR)¹⁷ as:

... any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability behaviour, location or movements.

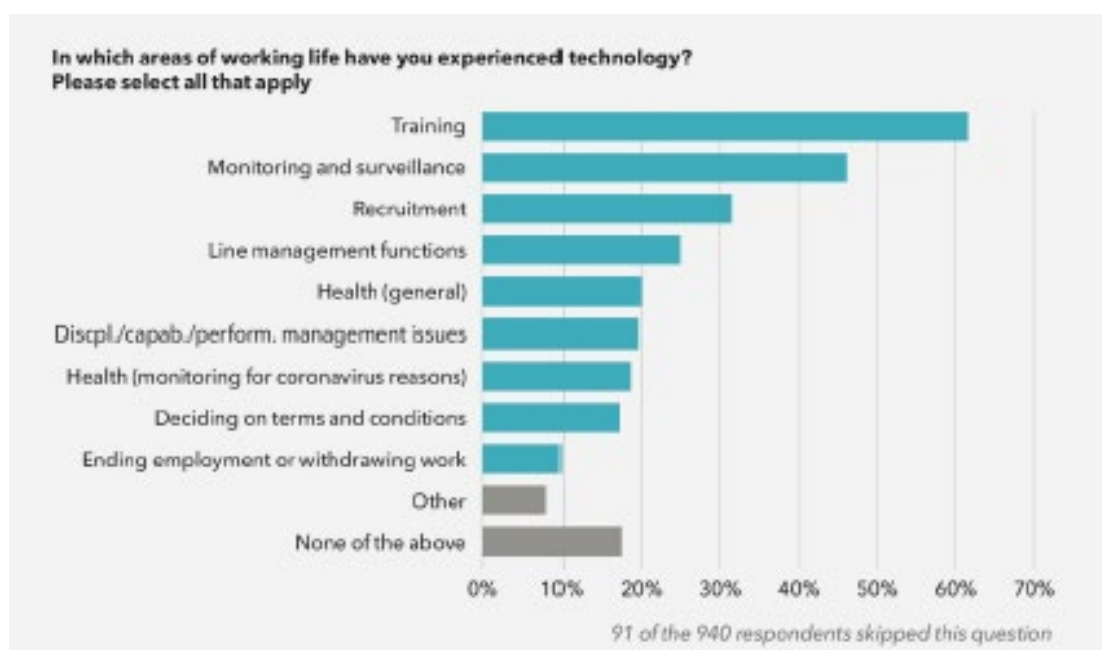
- 1.15. AI, ADM, and profiling are used in many ways, for example marketing, design and producing goods and services, and also in the management of workers and employees.
- 1.16. Some commentators argue that through profiling, “*a machine*” can make nuanced judgements about people, such as predicting the risk they will commit a crime or turn up late for work or move to a competitor, by analysing known and inferred personal data about that person. However, as we explain later, it can be an opaque process and susceptible to discrimination, even though it may be responsible for important decisions about people.

¹⁷ Note that post-Brexit, the GDPR, whilst an instrument of EU law, is part of a new body of retained EU law that has a continued existence: see [section 3 of the European Union \(Withdrawal\) Act 2018](#). In its retained form it is now called the [UK GDPR](#): see [The Data Protection, Privacy and Electronic Communications \(Amendments etc\) \(EU Exit\) Regulations 2019](#). The UK GDPR and the [Data Protection Act 2018](#) – also amended post-Brexit – create a single UK data protection regime.

The impact of Covid-19

The range of effects

- 1.17. AI, ML, ADM, and profiling have become more prevalent during the Covid-19 pandemic in many contexts, not just in relation to work. The focus of this Report is the world of work and here there has been a proliferation in use of AI technologies by employers seeking to grapple with the challenges of working both at home and in the workplace. This growth has been driven by several factors such as the need to police social distancing and minimise the ever-present threat of infection, and to maintain or improve productivity in the face of the huge economic pressures created by the pandemic.
- 1.18. If these issues were confined to a few limited contexts, then perhaps it would not have been necessary for the TUC to become so heavily engaged in thinking through how it should approach new technologies. However, the TUC's *Worker Experience Report* demonstrates that in the summer of 2020 these technologies were already being used on a very broad front, at each stage in the employment relationship from recruitment to dismissal. This chart, taken from the *Worker Experience Report*, shows the main areas of which the respondents to the survey were aware:



Fear and trust

- 1.19. Alongside this quantitative analysis, the *Worker Experience Report* discloses the range of impact these new technologies are having on workers and employees. The themes running through the main findings of the *Worker Experience Report* concern worker's fears and lack of trust. The *Worker Experience Report* noted that:
- Some employers have deployed new monitoring technologies as a result of the increase in homeworking created by the pandemic.
 - There is a perception that these new technologies are being used in an intrusive way which goes well beyond the type of monitoring that employees would experience in their usual working environments.
 - There is a strong feeling, from workers and union representatives alike, that technology is being deployed without their full knowledge or understanding.
 - There are concerns that AI-powered solutions can be flawed. For example automated absence-management systems were highlighted, which had wrongly concluded that employees were improperly absent from work leading to performance processes being incorrectly triggered.
 - Workers and employees had experienced poor mental health due to perceived unfairness driven by AI-powered technology.
 - Trade union representatives perceive that managers often do not understand AI-powered technology and perceive it to be unimpeachable.
- 1.20. To our own knowledge some employers used the scores attributed from unexplained automated online interviews of staff, conducted without human intervention, to determine who should be made redundant. From the perspective of employees who do not understand what has happened to them, we can begin to see the realisation of the fearful prospect of which Klaus Schwab warned.
- 1.21. The problem of lack of trust is not confined to the employment relationship but is evident in many other contexts in which AI systems are used. It has been

reflected in surveys that show trust in AI is now very low in the UK. The [Centre for Data Ethics and Innovation \(CDEI\)](#) published a [Barometer Report](#) on 23 June 2020 finding significant levels of lack of trust in AI. Since then, it has certainly deteriorated because of the controversy concerning the decisions made between Ofqual and the Department of Education during the summer of 2020.¹⁸ The fact that students were being “*marked*” by algorithm rather than human examiners suddenly alerted the public to the fact that life-changing decisions were being made about people “*by machines*” and not humans and for many this was unacceptable.

- 1.22. Some indication of the impact that this increased awareness has had on the public can be seen from a Report of [the British Computer Society](#) published on 22 September 2020 after the exam fiasco. It contained a familiar message:¹⁹

...the majority of people do not trust computers to make decisions about any aspect of their lives...

- 1.23. Whilst many organisations might be attracted to the idea of making large-scale decisions quickly and with as little human input as possible, events such as the 2020 exam debacle demonstrate the dangers of proceeding without a clear understanding of the importance of trust. Where trust is lacking there is bound to be a consequence. In our view, therefore, trust is not an issue to be dealt with as an afterthought; speedy decision-making is pointless if society does not trust the technology to deliver fairness and accuracy. Trust in such systems must be an aim from the outset. So, for the TUC, and indeed for all of us in any way connected with the world of work, the question is: How can it be ensured that the deployment of AI systems in the workplace can be trusted?
- 1.24. No less important is the question of whether this rapid automation of decision-making, that can so markedly affect the lives we live, is even ethical or at least

¹⁸ The Chair of Ofqual’s written statement to the Education Select Committee concerning the award of GCSE, AS, A levels in 2020 is [here](#).

¹⁹ The British Computer Society’s Report is [here](#).

always ethical. As with many technological developments in the past, discussions about the ethical implications of the development of AI systems has preceded discussion about legal regulation. These discussions are wide ranging and very important but eventually lead to the question of what regulation is necessary to ensure the benefits of the technology while avoiding its harms. That is the stage that has now been reached in the UK, in Europe and in the US.

- 1.25. Those discussions are taking place at both the general and specific level. It is very much hoped that this Report can contribute to the specific level of addressing the high-risk implications of uncontrolled deployment of AI systems in the world of work. These are real and pressing concerns both of substance and of process. If there is no trust in a system because it is not considered to be accurate, rational, non-discriminatory, proportionate, lawful, and ethical, its utility is hugely undermined.

The “always-on” culture

- 1.26. It might be thought that these new technologies would be liberating for workers, and in some ways they can be. But in and beyond the *Worker Experience Report*, and through meetings with the TUC’s AI Working Group, we have learned that the new technologies are encroaching significantly on workers’ private spheres over and above the proper limits of professional and working time. Increased digitalisation, through AI and other forms of technology, is contributing to an “always-on” culture in which employees are never completely free from work. There is a growing sense that employers are increasingly expecting their workforce to be easily contactable all times.
- 1.27. Research conducted by Aviva in the UK published in December 2020 has shown that these views are widespread. This research showed how 44% of surveyed employees felt that they never fully switched off from work, and 63% said that they regularly checked their emails outside of working hours.²⁰ The pandemic has led to an increase in employees feeling the need to check their emails. Some employers are seeking to create a culture amongst their staff of

²⁰ Aviva’s Report “*Embracing the Age of Ambiguity*” can be accessed [here](#).

being willing to communicate with management or colleagues regardless of whether this is outside their normal working hours.

- 1.28. We are concerned that the UK's politicians are being slow to take on board the implications of these changes. Press stories in January 2021 have suggested that the UK government is considering reform of many rights derived from EU law, such as the regulation of working time. Understandably this has led to increased fears within the union movement that workers will come under greater pressure to surrender their private time to the growing “*always-on*” culture.
- 1.29. We hardly need to spell out the mental health implications from the erosion of truly work-free time in people's lives. Everyone needs rest and a time away from the pressure of work, regardless of their position. It is therefore important that AI technologies are regulated to ensure they do not encroach upon the private lives of employees and workers.

Concerned bodies

- 1.30. That said, these kinds of issues have not been entirely ignored. There are some specialist UK bodies considering the impact of AI and ADM that have at least started to consider their effect on the workplace. These include the CDEI,²¹ the House of Commons Science and Technology Committee,²² the All-Party Parliamentary Group on Artificial Intelligence (APPG AI),²³ the Information Commissioner's Office (ICO),²⁴ the Equality and Human Rights Commission

²¹ The CDEI's [“Review into bias in algorithmic decision-making”](#) was published in November 2020.

²² The House of Commons Science and Technology Committee released a Report, [“Algorithms in decision-making”](#), Fourth Report of Session 2017-19, on 23 May 2018, which examines the use of AI and ADM in a variety of areas including recruitment and more generally the risk around bias.

²³ The APPG AI has published many Reports including a July 2020 document entitled, [“Face and Emotion Recognition: How can regulation protect citizens and their privacy?”](#) which touches upon the use of biometric data in recruitment.

²⁴ The ICO is the UK's independent authority set up to uphold, amongst other matters, information rights in the public interest. It has produced material concerning the use of AI, some of which focuses on the employment relationship. It has published key documents such as [“Big data, artificial intelligence,](#)

(EHRC),²⁵ the Advisory Conciliation and Arbitration Service (ACAS),²⁶ the Commission on Workers and Technology chaired by Yvette Cooper MP,²⁷ the Committee on Standards in Public Life (CSPL),²⁸ and the Alan Turing Institute.²⁹

- 1.31. There are also important NGOs that have considered the impact of automation and AI on the future of work such as the Royal Society,³⁰ the Institute for the Future of Work (IFOW),³¹ the British Computer Society³² and the Chartered Institute of Personnel and Development (CIPD).³³ Much work is also being done at the international level, some of which we shall note in the rest of this Report. The *Worker Experience Report* makes a major contribution to this work.
- 1.32. Even though we all hope the pandemic will abate, it seems likely that the changes introduced during 2020 and 2021 will have a lasting impact on the

[machine learning and data protection](#), its recent document [“Guidance on the AI auditing framework: Draft guidance for consultation”](#), [“The employment practices code”](#) and material under the banner [“Coronavirus recovery – data protection advice for organisations”](#). Most recently, in December 2020, it produced a short guide entitled, [“Six things to consider when using algorithms for employment decisions”](#).

²⁵ The EHRC has hosted events bringing together key actors in civil society in order to discuss ways of tackling algorithmic discrimination and published a useful [“Algorithms and artificial intelligence reading list”](#).

²⁶ ACAS has published an independent paper entitled, [“My boss the algorithm: an ethical look at algorithms in the workplace”](#).

²⁷ More information about the Commission on Workers and Technology chaired by Yvette Cooper MP and hosted by the Changing Work Centre – a joint research initiative from Community and the Fabian Society is available [here](#).

²⁸ The CPSL addressed AI in its document [“Artificial Intelligence and Public Standards”](#).

²⁹ The Alan Turing Institute recently held an event entitled, [“Tackling the challenges of Intelligence analysis with workplace productivity software”](#) and has published articles examining digitalisation and data collection as a means of promoting workers’ rights e.g. [“Can African and Asian workers challenge exploitation in the gig economy?”](#).

³⁰ The Royal Society commissioned a Report from Frontier Economics entitled, [“The Impact of Artificial Intelligence on Work: An evidence review prepared for the Royal Society and the British Academy”](#).

³¹ More information about the Institute for the Future of Work (IFOW) is available [here](#).

³² See <https://www.bcs.org/>

³³ See the CIPD Report [“Workplace technology: the employee experience”](#).

world of work. That is a further reason why we think it essential *now* to step back for a moment to reflect on whether and, if so, how adequately our current legal system can respond.

The UK's Labour Law code and related provisions

- 1.33. It is one thing to note these problems and another to consider how they should be addressed. Some of them can be addressed by argument and discussion about standards and best practice. Some might be addressed by collective bargaining. Yet in the end it is through good and effective laws that abuses are ultimately stopped.
- 1.34. In the next Chapter we shall discuss the extent to which, what we shall call the UK's Labour Law Code,³⁴ has the power to stop abuses, and to promote the necessary trust in AI systems. In the next section of this Chapter, we shall identify some key aspects of the collection of laws and regulations and common law principles that make up this body of law. We start here because, as has rightly been said, "*the vital function*" of labour law is to limit an employer's powers and to protect the human dignity of employees and workers.³⁵ This discussion proceeds in two sections because the rules and regulations of modern UK Labour Law have two sources: partly they are based on the

³⁴ This is ordinarily understood to mean the legislation that supports the common law principles: the Equality Act 2010, the Equal Pay Act 1970, the Sex Discrimination Act 1975, the Race Relations Act 1976, the Trade Union and Labour Relations (Consolidation) Act 1992, the Disability Discrimination Act 1995, the Employment Rights Act 1996, the Working Time Regulations 1998, the National Minimum Wage Act 1998, the Transnational Information and Consultation of Employees Regulations 1999, the Part-time Workers (Prevention of Less Favourable Treatment) Regulations 2000, the Fixed-term Employees (Prevention of Less Favourable Treatment) Regulations 2002, the Employment Equality (Sexual Orientation) Regulations 2003, the Employment Equality (Religion or Belief) Regulations 2003, the Information and Consultation of Employees Regulations 2004, the Occupational and Personal Pension Schemes (Consultation by Employers and Miscellaneous Amendment) Regulations 2006, the Employment Equality (Age) Regulations 2006, the Transfer of Undertakings (Protection of Employment) Regulations 2006. Statutory Codes of Practice made under this and connected legislation should also be included.

³⁵ See De Stefano, V., 2019, "*Negotiating the Algorithm: Automation, Artificial Intelligence, and Labor Protection*", International Labour Organisation, Employment Policy Department Working Paper No. 246, see [here](#).

development of the common law of “*master and servant*” as it was once called, and partly on a series of legislative measures, enacted piecemeal over many years to address specific problems where the common law was considered to be inadequate.

The Common law

Mutuality

- 1.35. AI systems are often introduced to do jobs that humans would have done or might have done. The consequence is that employees are being made to have more of a “relationship” with these machines and less with the humans who would otherwise have carried out such functions. This has implications because all discussion of these laws must start with the fact that the common law relationship between employer and employee involves a **mutual** contract in which the employee’s promise to work is mutually dependent on the employer’s promise to pay the employee.
- 1.36. This mutuality of obligation is a special feature. Mutuality is not a general requirement in contracts; other contracts can be made without mutual terms but not those contracts that define an employment relationship. In these, the mutuality of obligation – “*I will do this for you if you do that for me*” – is always present. We are emphasizing this because it gives rise to some features that engage directly with the kinds of problems these new technologies are throwing up.³⁶

Personal service

- 1.37. First, this mutuality goes hand in glove with the employee’s obligation of **personal service**.³⁷ If there is no obligation of personal service then the contract

³⁶ See more generally the discussion on the transformation from master and servant to modern labour law in Deakin, S. and Morris, G.S., *Labour Law*, 2012, Hart.

³⁷ This characterisation of the relationship as “*personal*” is not new. It is the reason why the courts have never forced the parties of contracts of employment to continue to work together by orders for specific

is not considered to be one of employer and employee; it is just another commercial relationship and outside the scope of this Report. This personal relationship entails important consequences; for instance, an employee cannot simply substitute another to do his or her work if he or she does not wish to turn up for work. Likewise, the employer cannot simply transfer the employee or worker to another employer without specific agreement and permission of the employee.

Trust and confidence

- 1.38. This personal relationship is also the reason why the highest courts have held that every employment contract is subject to an implied term of mutual trust and confidence. In 1997, in a famous judgment in the House of Lords in [Malik and Mahmud v. Bank of Credit and Commerce International S.A.](#),³⁸ Lord Steyn described this obligation, saying:³⁹

The employees ... rely on a standardised term implied by law, that is, on a term which is said to be an incident of all contracts of employment: *Sally v. Southern Health and Social Services Board* [1992] 1 A.C. 294, 307B. Such implied terms operate as default rules. ... It is expressed to impose an obligation that the employer shall not:

performance. The extent of this obligation has been tested in many recent cases concerning the gig economy, yet in none of them has it been doubted that personal service lies at the heart of this kind of relationship. Personal service is an aspect of not only of what are properly called employment contracts but also many contracts of “gig” workers: [section 230\(3\) of the Employment Rights Act 1996](#) and see *Uber BV & Ors v Aslam & Ors* [2021] UKSC 5, see [here](#).

³⁸ For instance the nature of the default term has been discussed in the judgments of Lords Nicholls and Steyn giving the judgments of the House of Lords in *Malik and Mahmud v. Bank of Credit and Commerce International S.A.* [1997] UKHL 23; [1998] AC 20; [1997] 3 All ER 1; [1997] IRLR 462; [1997] 3 WLR 95; [1997] ICR 606, see [here](#).

³⁹ With which Lords Goff of Chieveley, Mackay of Clashfern and Mustill specifically agreed. Lord Nicholls gave a consistent judgment.

"... without reasonable and proper cause, conduct itself in a manner calculated and likely to destroy or seriously damage the relationship of confidence and trust between employer and employee."⁴⁰

The evolution of the term is a comparatively recent development. The obligation probably has its origin in the general duty of co-operation between contracting parties: B.A. Hepple, *Employment Law*, 4th ed. (1981), paras. 291-292, pp. 134-135. The reason for this development is part of the history of the development of employment law in this century. The notion of a "master and servant" relationship became obsolete. Lord Slynn of Hadley recently noted

"the changes which have taken place in the employment and employee relationship, with far greater duties imposed on the employer in the past, whether by statute or judicial decision, to care for the physical, financial and even psychological welfare of the employee": *Spring v. Guardian Assurance Plc.* [1995] 2 AC 296, at 325B.

The major importance of the implied duty of trust and confidence lies in its impact on the obligations of the employer: Douglas Brodie, "Recent cases, Commentary, The Heart of the Matter: Mutual Trust and Confidence" (1996) 25 I.L.J. 121. And the implied obligation as formulated is apt to cover the great diversity of situations in which a balance has to be struck between an employer's interest in managing his business as he sees fit and the employee's interest in not being unfairly and improperly exploited.

- 1.39. The term has been discussed in many cases since then. There is no doubt that it is essential for a contract of employment to be effective; Lord Justice Mummery neatly explained this in [Keen v Commerzbank AG](#)⁴¹ saying:

43. The employment relationship contains implied duties which do not normally feature in commercial contracts sued on by business men ...

⁴⁰ He added "See *Woods v. W.M. Car Services (Peterborough) Ltd.* [1981] I.C.R. 666, 670 (Browne-Wilkinson J), approved in *Lewis v. Motorworld Garages Ltd.* [1986] I.C.R. 157 and *Imperial Group Pension Trust Ltd. v. Imperial Tobacco Ltd.* [1991] 1 W.L.R. 589. A useful anthology of the cases applying this term, or something like it, is given in Sweet and Maxwell's *Encyclopedia of Employment Law*, (Loose Leaf ed.) Vol. 1, para. 1.507, pp 1467-1470."

⁴¹ [2006] EWCA Civ 1536, [2007] IRLR 132, [2006] 2 CLC 844, [2007] ICR 623, see [here](#).

Employment is a personal relationship. Its dynamics differ significantly from those of business deals and of state treatment of its citizens. In general there is an implied mutual duty of trust and confidence between employer and employee. Thus it is the duty on the part of an employer to preserve the trust and confidence which an employee should have in him. This affects, or should affect, the way in which an employer normally treats his employee.

The implications of trust and confidence between employer and employee

- 1.40. The common law has always recognised that the absence of this trust and confidence is fatal to the success of any employment contract; in its absence the only possible remedy is to treat the main obligations of the contract as at an end because the courts recognise that you cannot force mutual trust and confidence between two parties. Where this happens, employees can sue for breach of contract and (subject to certain other statutory conditions) bring constructive unfair dismissal claims.
- 1.41. In our view this obligation of mutual trust and confidence has other important consequences for any analysis of the implications of AI systems on the workplace.
- 1.42. First, as Lord Justice Mummery went on to say in *Keen*, it means that employers are very often under an obligation to **provide explanations** to employees for certain decisions where the employer exercises discretions under the contract of employment (*Keen*, paragraph 44). In the same case, Lord Justice Moses pointed out that if it were otherwise it could lead to exploitation (*Keen*, paragraph 110).
- 1.43. Second, the common law recognises that there is a **power imbalance** inherent in the relationship which has implications. Chief among these is that an employer is required to take decisions about employees in way that is **lawful, rational** and in **good faith**. Lady Hale explained this in *Braganza v BP Shipping Limited*⁴² saying:

⁴² [2015] UKSC 17, [2015] IRLR 487, [2015] ICR 449, [2015] 1 WLR 1661, see [here](#).

18 ... the party who is charged with making decisions which affect the rights of both parties to the contract has a clear conflict of interest. That conflict is heightened where there is a significant imbalance of power between the contracting parties as there often will be in an employment contract. The courts have therefore sought to ensure that such contractual powers are not abused. ...

32 ... The particular context of this case is an employment contract, which, as Lord Hodge explains, is of a different character from an ordinary commercial contract. Any decision-making function entrusted to the employer has to be exercised in accordance with the implied obligation of trust and confidence.

- 1.44. Third, it means that the actions of employers can be subject to closer **scrutiny** than the parties to a simple commercial contract (*Braganza*, paragraph 55).
- 1.45. As we will explain in [Chapter 2](#), employers deploying AI systems will sometimes make decisions that impact in a fundamental way on their employees and their livelihood, such as decisions about disciplinary action or dismissal. It might be thought that because a machine has made a decision this changes things, but this is not so. The use of AI and ADM does not abrogate employers from the obligation to make such decisions to a high standard.

The legislative framework

- 1.46. Just as for the common law, the legislative measures that have been added to define better the legal rights of employers and their employees and workers have not been altered just because new technology is being deployed.

Statutory rights to fair process

- 1.47. For instance, the employer's statutory obligation to **act fairly** in terms of **process** and **outcome** when dismissing employees with over two years'

continuous service remains.⁴³ It is not watered down in any way just because business has utilised new ways for human resource management.

Health and safety

- 1.48. There are many other legislative provisions that are relevant. One such class of provisions, which have been introduced precisely because of the power imbalance between employer and employee, includes those statutory provisions designed to help protect health and safety in the workplace.⁴⁴

Equality

- 1.49. We discuss in [Chapter 2](#) how new forms of technology can create discrimination as well as replicate and embed existing discrimination through the ML process. So, it is important to note that the class of legislative protection based on the fundamental right of all employees to **work without discrimination** in relation to the protected characteristics such as race, sex, sexual orientation etc has not been altered just because there have been technological changes.

Data protection and privacy rights

There are also important measures not limited to the world of work that are nonetheless very important in that context. Thus, we all have rights to be protected in relation to data processing. These rights are contained in the UK in the Data Protection Act 2018 (**DPA**), passed to give effect to the General Data Protection Regulation, now known following Brexit as the UK GDPR, and based on the general principle that data should be accurate and processed in a way that is fair and transparent.⁴⁵

- 1.50. Article 1 of the UK GDPR emphasises the critical importance of data protection rights in the UK, stating that the purpose of the regulation is to protect:

⁴³ See Part X of the Employment Rights Act 1996, see [here](#).

⁴⁴ Including the Health and Safety at Work Act 1974, numerous regulations specific to particular workplaces, and the Working Time Regulations 1998 SI 1998 No. 1833.

⁴⁵ The Information Commissioner's Office guide to the UK GDPR is [here](#).

... fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data ...

Privacy

- 1.51. Similarly, employees and workers continue to enjoy a right to privacy pursuant to Article 8 of the European Convention on Human Rights (**ECHR**) and the Human Rights Act 1998 (**HRA**). Article 8 states:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

- 1.52. All rights to privacy are not lost the moment a person engages in a contract of personal service. This right is not derived from membership of the European Union and has not been lost following Brexit. So, an employee's decision to enter into a contractual relationship with an employer does not mean that they sacrifice their entitlement to a private virtual or physical space but retain a reasonable expectation of privacy at work.⁴⁶

Collective rights and obligations

- 1.53. In [Chapter 2](#) and [Chapter 3](#), we shall discuss how we can ensure that AI and ADM are used appropriately by, for example, harnessing the power of collective bargaining and through the collation of worker data. We also

⁴⁶ *Halford v United Kingdom* 3 BHRC 31, (1997) 3 BHRC 31, (1997) 24 EHRR 523, 24 EHRR 523, [1997] ECHR 32, [1998] Crim LR 753, [1997] IRLR 471, see [here](#).

consider later in this Report how AI has been used to undermine union rights. These issues engage with those aspects of the modern employment relationship concerned with collective rights and obligations. These will be of great importance to the TUC since its basic premise is that workers' interests can be better represented through collective representation.

- 1.54. As will already be well known, Article 11 ECHR and the HRA 1998 give every person the **right to associate**, including the right to join a trade union. This right to associate includes the right for trade unions to be heard and to pursue their members' interests as well as the **right to bargain collectively**.⁴⁷

The special status of workers

- 1.55. So far in this Report we have not made any broad distinction between workers who, like employees, also have obligations of personal service. The status of worker does differ from that of an employee in that the mutuality obligations are different, *but* many fundamental rights are the same, including rights not to suffer discrimination, rights in relation to data processing, and rights in relation to privacy. What can be said in relation to the differences between their status is that if anything workers have an *additional* need for protection to ensure that AI and ADM are used appropriately. Their less-protected status under the UK's Labour Code, for example the absence of unfair dismissal rights for workers, renders them more vulnerable to poorly deployed technology in the workplace.

"Red line" limits to the use of AI and ADM in the workplace

- 1.56. Reflecting on this analysis so far, we are clear that some uses of AI systems are simply not acceptable in our society; they are wholly contrary to central aspects of the modern employment relationship that we have described above. Such uses do not respect the personal relationship central to the nature of employment and worker status; rather, they lead to exactly the kind of

⁴⁷ See for instance *Demir v Turkey*, [2009] I.R.L.R. 766, (2009) 48 E.H.R.R. 54, see [here](#).

alienation and robotisation that Klaus Schwab foresaw as such a serious risk in his prophetic words set out in the Introduction to our Report.

- 1.57. In the bullet points in the box below, we have set out where we think the *red lines* should be drawn. While we recognise that the text of these points might be discussed, the key point is that each expresses a limit based on the fundamental and essential elements of the modern employment relationship that we have outlined.

"Red lines" beyond which the deployment of new technologies should not occur

- Employers should only be permitted to use AI and ADM to make important, high-risk decisions, about existing or potential employees and workers, where those decisions can be sensibly explained and understood by employees.
- Employers, and their agents, should not process the data of employees, workers and job applicants in a way which amounts to discrimination as understood within UK law.
- Employees, workers, and their representatives should be part of the decision-making process undertaken by employers when determining the use of AI and ADM to make important decisions about the workforce.
- Existing and potential employees and workers should readily be able to know what AI and ADM systems are being used in the workplace; the information should be available in easily accessible and intelligible form.
- Existing and potential employees and workers should have access to sufficient information about the way in which AI and ADM operates in the context of the employment relationship to be able to satisfy themselves that the technology is being used in a way which is accurate, rational, non-discriminatory, proportionate, lawful, and ethical.

- 1.58. We recommend that the TUC should state that the national recognition and adoption of these “*red lines*” is a fundamental policy. The precise way that they should be applied will of course require internal debate and discussion with others. The key point is that these form a baseline from which all discussion about how AI systems used in the work context should be comprehensively regulated by the law.
- 1.59. In our view it is urgent that these “*red lines*” are universally acknowledged as a baseline. The deployment of these new technologies has already proceeded far and, every day, the economic, commercial, and political pressure grows to go further. We do not think that there is any time to waste in standing up to that pressure.
- 1.60. If the TUC takes our advice, then it will need to develop a strategy around five further related key questions, central to the issue as to how these red lines can be made effective:

- How can it be ensured that AI and ADM are consistent with and respectful of the modern employment relationship and these “*red lines*”?
- What are the limits of the existing UK Labour Code and data protection and other laws in achieving this aim?
- What legislative changes are needed to ensure that these are fit for this purpose?
- Does the structure of the justice system help or hinder the protection of workers’ rights in a world shaped by technology?
- What can the trade union movement do to ensure that employees and workers’ rights are not sacrificed in the Fourth Industrial Revolution?

- 1.61. In the next Chapters of our Report, we explain our answers to these questions, starting in [Chapter 2](#) with an analysis of the ways in which AI, ML and ADM can threaten the modern employment relationship whilst exploring the extent to which the existing legal framework provides adequate protection.
- 1.62. Thereafter, in [Chapter 3](#), we set out our proposals as to how the TUC might develop a strategy of engagement with these issues, including both proposals for reform and recommendations for specific legal and practical steps that can be taken now so as to ensure that the legal system in the UK remains “*fit for purpose*” and respects the “*red lines*” that we have articulated above.

Chapter 2 – The capacity of UK laws to control the use of AI systems in the workplace

Summary

In this Chapter we explore the ways in which AI systems can affect typical modern employment relationships and the more precarious position of workers with personal relationships with employers. We shall use case studies, derived from academic and other research and other publicly available sources, as well as information collected by the TUC in the *Worker Experience Report*, to identify typical effects, and then to analyse the legal rights and principles that are engaged.

Although our analysis shows that the current laws are by no means completely ineffective to control AI, ML and ADM, it also shows there are many significant gaps that need to be addressed. In this Chapter we set out 15 separate conclusions, listed under 8 headings, based on specific legal rights (marked A to H), as to where and how deficiencies exist. For convenience we set all our conclusions out here together; the explanation for each conclusion is provided below.

| | |
|---|---|
| A | <u>Right to work without discrimination</u> |
| | Conclusion 1: AI, ADM and profiling can discriminate. The existing legal framework giving effect to the principle of non-discrimination in the workplace is in principle capable of tackling discriminatory uses of AI and ADM but can only be used effectively where transparency is guaranteed. |
| | Conclusion 2: There are difficulties with identifying when and how and by whom discrimination is introduced within the “ <i>value chain</i> ” of actors who have created an AI tool, which in turn can make it difficult for workers and employees to enforce rights to non-discrimination. |
| B | <u>Principles of observability and transparency</u> |

| | |
|---|--|
| | <p>Conclusion 3: The existing legal framework does not adequately compel observability and transparency around the use of AI and ADM. There is no universal legal right of “<i>explainability</i>”, and no recognised entitlement to a personalised explanation. This is problematic as applications of AI, ML and ADM in the workplace can have significant legal implications for people such as the risk of discrimination.</p> |
| | <p>Conclusion 4: Intellectual property rights, and their protection under international trade agreements, have the potential to impede the degree of transparency necessary to ensure the lawful and ethical use of AI and ADM. This must not be allowed to happen as it will make an existing difficulty in holding AI systems to account even more difficult.</p> |
| C | <p>Right to privacy</p> |
| | <p>Conclusion 5: Article 8 ECHR is adequate to protect the privacy of employees and workers from intrusive forms of AI and ADM. However, at present there is inadequate legally binding guidance to employers explaining when Article 8 rights are infringed by the use of AI-powered technology and how, practically speaking the Article 8 balancing exercise is to be resolved. Without such guidance employers will not fully understand their obligations, nor will employees be able to hold the line against inappropriate incursions into their right to a private life.</p> |
| D | <p>Right to data protection</p> |
| | <p>Conclusion 6: The data protection framework contained in the UK GDPR and the DPA 2018 has the potential to provide valuable protection to workers and employees in that data can be processed only on certain specified grounds. However, one lawful basis for data processing by an employer is that it is “necessary” for the performance of the employment contract (UK GDPR, Article 6(1)(b)). Unless this ground is carefully defined, which at present it is not, there is a substantial risk that all data processing within the employment relationship will be treated as consistent with the UK GDPR.</p> |

| | |
|---|--|
| | <p>Conclusion 7: A further lawful basis for data processing is that it is necessary for the purposes of a legitimate interest, provided this is not overridden by the fundamental rights of the employee (UK GDPR, Article 6(1)(f)). Unless this ground is carefully defined, which at present it is not, there is a risk that all data processing within the employment relationship will be treated as consistent with the UK GDPR.</p> |
| | <p>Conclusion 8: The data protection framework contained in the UK GDPR has the potential to provide valuable protection to workers and employees in that, dependent on the lawful basis for the processing, there is a right not to be subject to fully automated decision-making (Article 22) and a right to object (Article 21). However, since the lawful basis of data processing under Article 6 dictates the availability of these rights, the lack of clarity around Article 6 creates serious uncertainty about the scope of workers' rights.</p> |
| | <p>Conclusion 9: The important rights in Article 21 and Article 22 of the UK GDPR are subject to various exceptions, which are insufficiently defined. The lack of clarity creates serious uncertainty about the scope of workers' rights.</p> |
| E | <p><u>Protection from AI-powered decisions that are irrational or unfair</u></p> |
| | <p>Conclusion 10: Unfair dismissal legislation should protect employees who qualify for protection under s.97 and s.98 of the Employment Rights Act 1996 from dismissal decisions that are factually inaccurate or opaque in the usual way. The use of AI-powered tools to support such decisions does not make any difference to this important legal protection.</p> |

| | |
|---|---|
| | <p>Conclusion 11: Alongside unfair dismissal rights for employees with two years' continuous service, there is some protection for employees and workers who are subject to decisions that have been informed by inaccurate data and /or data processing in that all personal data which is processed as part of an AI-powered technology or ADM must be accurate (Article 5(1)(d), UK GDPR). These rights could be sued on in the event of disciplinary action or other detrimental treatment arising from the use of AI. However, unfair dismissal rights are not universal, and the UK GDPR cannot be sued on in the relatively cheap and accessible Employment Tribunal, meaning that there are gaps in effective legal protection.</p> |
| F | <p><u>Management within a personal relationship</u></p> |
| | <p>Conclusion 12: The personal nature of the employment relationship is threatened if there is no entitlement for employees to insist that certain decisions are made about them by a human being as opposed to being fully automated. Equally, workers are exposed where decisions that require empathy and a "<i>human touch</i>" are made about them by an algorithm. Further, for some employees and workers, technology is difficult for them to access, use or understand. The failure to provide these groups with access to a human decision-maker will lead to marginalisation.</p> |
| G | <p><u>Protection of workers' private time from the intrusion of technology</u></p> |
| | <p>Conclusion 13: The increased use of technology is encroaching more on workers' lives, leading to a slow erosion of the distinction between work and private time due to the ease with which communication can take place. There is no existing legal tool in the UK that creates a positive right to enforce boundaries around communication during the personal life of an employee or worker, which may otherwise be eroded by technology.</p> |

| | |
|---|--|
| H | Rights of association and bargaining |
| | Conclusion 14: AI and ADM pose a significant risk to the welfare of the workforce. However, existing legislation does not mandate collective bargaining in relation to their use. Consultation and a right to collective bargaining in relation to their introduction and use is necessary to promote trust, avoid abuses and secure its beneficial use. |
| | Conclusion 15: There is adequate legal protection in relation to the preservation of trade union activities. However, these rights will be enforceable only in so far as there are meaningful obligations in relation to transparency concerning AI, ADM, and related technologies. |

A: Right to work without discrimination

- 2.1. The right to equal treatment and non-discrimination is a fundamental principle given specific effect in Great Britain by the [Equality Act 2010](#), and in Northern Ireland by cognate provisions. It is a right enjoyed by job applicants, employees, and workers, both while the contract is on foot, and to some extent even after the working relationship has ended. All job applicants, employees and workers are entitled to work free from discrimination, harassment and victimisation relating to defined protected characteristics: age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, and sexual orientation.⁴⁸
- 2.2. Although commentators have shown for some time that AI systems give rise to discrimination, bias resulting from AI systems continues to occur.⁴⁹ We need to analyse first how this can happen before discussing what should be done to establish effective legal protections to prevent it happening in the workplace.

⁴⁸ See [Chapter 1](#) of the Equality Act 2010.

⁴⁹ See for instance in the UK [“Review into bias in algorithmic decision-making”, 2020, Centre for Data Ethics and Innovation](#). Similar conclusions have been reached in other European countries and in the United States.

How bias can occur in AI systems

- 2.3. We are all familiar with the problem of humans stereotyping individuals and acting on the stereotype rather than the facts of the case. **Something similar can often happen with AI systems.** An example of a way in which this kind of bias can enter AI systems is demonstrated by some recent work undertaken by journalists in the US in an organisation called [ProPublica](#). Although the example concerns the criminal system it well exemplifies a problem that can easily occur in the context of work.
- 2.4. **The researchers noted that in some states, judges were making sentencing decisions in criminal cases in part by reference to the output from an AI system called Correctional Offender Management Profiling for Alternative Sanctions (COMPAS).⁵⁰ These outputs purportedly predicted the likelihood that an individual would commit a violent crime in the future. The system purported to look at historic data about past cases to make these predictions when confronted with the data relating to a specific new case.**
- 2.5. The ProPublica journalists were concerned to see if the COMPAS system was fair; to this end they analysed 7,000 COMPAS “*risk scores*”, finding that they were nearly twice as likely to predict *falsely* that black defendants would be criminals in the future in comparison to white defendants.⁵¹ **They concluded that the algorithm appeared to have “*learnt*” a false discriminatory correlation between race and the likelihood of committing crime. They concluded that the source of the problem lay in the data that had initially been used to train the system. This data was subject to a process of ML to enable COMPAS to use the historic data to make predictions about the future conduct of offenders.**

⁵⁰ It bears some similarity to a system used in the UK known as the “*Offender Assessment System*” (“OASys”), see [here](#).

⁵¹ Angwin, J., Larson, J., Mattu, S. and Kirchner, L., 2016, Machine bias risk assessments in criminal sentencing, see [here](#). ProPublica 2016.

- 2.6. ProPublica concluded that, far from creating an objective tool to facilitate judicial decision-making, COMPAS appeared to perpetuate discrimination.⁵² Biased training is a perennial problem with AI systems; the training data sets used as the basis of ML are rarely neutral. As a result, discriminatory correlations are “*learnt*” by the AI system when the algorithms work out how to replicate (biased) decisions made by humans contained in the training set of data. The AI system just creates a new stereotype.

The implications of biased AI systems

- 2.7. This is just one example of the kinds of biased decision-making that can occur as a result of AI systems being used without appropriate consideration as to their creation and output.⁵³ How might such bias be significant in the world of work? There are many different ways, but we shall start by looking at the recruitment stage.⁵⁴
- 2.7.1. Algorithms are used to target job adverts to certain groups, or to ensure application forms and CVs are automatically “*scraped*” for key information. They use historic data to look for likely candidates.
- 2.7.2. They are used to undertake background checks and to ensure that a potential applicant’s social media data is analysed.
- 2.7.3. Chatbots run by AI systems then conduct interviews and algorithms score performance within interviews including by analysing biometric data like appearance, presentation, and voice.

⁵² Its evidence was reviewed by the Wisconsin Supreme Court in an [Opinion of the 13 July 2016](#) in an appeal case called [State v. Eric L. Loomis](#), 881 N.W.2d 749 (Wis. 2016), cert. denied, 137 S.Ct. 2290 (2017).

⁵³ The CDEI Bias Review (op. cit.) has an extensive analysis of the different kinds of bias.

⁵⁴ See for instance [AI-assisted recruitment is biased. Here’s how to make it more fair](#), World Economic Forum 2019.

- 2.8. We will demonstrate some of the discrimination issues that can arise within these types of recruitment processes within **Case Studies A** and **B** below but first we must set out some provisions of the Equality Act 2010.

The Equality Act 2010

- 2.9. The Equality Act 2010 provides a three-stage process for determining if there is unlawful discrimination. First it defines the “*Protected Characteristics*” set out above. Next, the Equality Act 2010 defines what is “*Prohibited Conduct*” in relation to these Protected Characteristics,⁵⁵ of which direct and indirect discrimination and harassment (and a failure to make reasonable adjustments in the context of disability) will be the most significant.⁵⁶ The third stage is to define when Prohibited Conduct is unlawful. A fourth stage, which we do not need to discuss in this Report, concerns exemptions and defences.
- 2.10. One form of Prohibited Conduct is indirect discrimination, and this is likely to be very important where AI technology is concerned. Section 19 Equality Act 2010 defines indirect discrimination in the following terms:

⁵⁵ Prohibited Conduct is made unlawful on a largely, but not an entirely, similar basis for each of the Protected Characteristics. Some exceptions are provided for in relation to specific contexts. Provisions are also made that permit positive action and other specific steps to advance equality.

⁵⁶ In relation to the protected characteristic of disability there are also certain conducts that are prohibited on grounds specific to disability, such as the failure to make reasonable adjustments.

- (1) A person (A) discriminates against another (B) if A applies to B a provision, criterion or practice which is discriminatory in relation to a relevant protected characteristic of B's.
- (2) For the purposes of subsection (1), a provision, criterion or practice is discriminatory in relation to a relevant protected characteristic of B's if –
- (a) A applies, or would apply, it to persons with whom B does not share the characteristic,
 - (b) it puts, or would put, persons with whom B shares the characteristic at a particular disadvantage when compared with persons with whom B does not share it,
 - (c) it puts, or would put, B at that disadvantage, and
 - (d) A cannot show it to be a proportionate means of achieving a legitimate aim.

- 2.11. Ordinarily lawyers think of indirect discrimination claims as arising where an organisation, like an employer, adopts a rule that puts protected people at a disadvantage, for example a requirement to perform a certain job full time can put women who often have the primary responsibility for child-caring at a disadvantage.
- 2.12. We consider, however, that an algorithm, which is after all a “logical” rules-based process, can also be seen as a “*provision, criterion or practice*” (**PCP**) within the meaning of section 19 (1) Equality Act 2010.⁵⁷ Likewise, we consider that the database used to train ML algorithms or assist with semi- or fully-automated decision making is also likely to be conceptualised as a PCP by the courts and therefore fall under section 19 (1) Equality Act 2010.

⁵⁷ Although there isn't yet any case law which confirms that an algorithm or the training data used in the ML process can amount to a PCP, we are clear that this analysis is consistent with the [Code of Practice](#), approved by Parliament and issued by the Equality and Human Rights Commission (EHRC).

- 2.13. We shall consider now how these provisions might be significant in the context of AI systems.

Case Study A: Online job advertising marginalising female candidates

- 2.14. In this **Case Study A** we consider how a biased system can be analysed.

A global social media platform sells advertising space to its customers. Its selling point is that it uses sophisticated ML algorithms to target its client's adverts so as to maximise the number of people who pay attention to the advertisement. To achieve this aim, adaptive algorithms process vast amounts of data collated by the social media platform including behavioural data. This learning process is largely unsupervised. One corporate customer contracts with the social media platform in order to advertise a science, technology, engineering and mathematics (STEM) role. The job advert is "*neutral*" in that it has not been crafted, expressly or implicitly, to appeal more to men or women. Despite this, the job advert is significantly more likely to be shown to men. Specifically, men saw this ad 20% more often than women and younger women were even less likely to see the advert.

- 2.15. **Case Study A** can be readily analysed as an indirect discrimination claim.⁵⁸ The adaptive algorithm that led to women being shown the STEM advert less frequently than men is a PCP. The data set that has been used to train the adaptive algorithm in such a way as to create this outcome can also be conceptualised as an additional PCP. These PCPs separately or cumulatively place women at a "*particular disadvantage*" within the meaning of section 19(2)(b) Equality Act 2010 since they are less likely to see the STEM advert. A woman who would have applied for the STEM role but was denied the

⁵⁸ In **Case Study A**, there is also the potential for a direct sex discrimination under the Equality Act 2010 on the basis that the adaptive algorithms mean that women are at a greater risk of missing out on seeing a job advert than their male counterparts adopting the analysis in the Supreme Court decision of *R (on the application of Coll) v Secretary of State for Justice* [2017] UKSC 40. In other cases, the less-favourable treatment is the higher risk level experienced by women that does apply to men.

opportunity to do so since she was not shown the advert, would be able to bring herself within section 19(2)(c) Equality Act 2010.

- 2.16. This, however, is not the end of the analysis since there is always the potential under section 19(2)(d) Equality Act 2010 to justify indirect sex discrimination.
- 2.17. There are three steps that must be completed to establish a successful justification defence. It must be shown that there is:
- **A legitimate aim:** First, the measure adopted by the employer/service provider must be underpinned by a “*legitimate aim*”.
 - **Effectiveness:** Next, the measure must be capable of achieving the aim.
 - **Proportionality:** The measure used must also be proportionate. It is critical to note that in almost all cases a measure will *not* be proportionate where the aim could be achieved through a different measure that was less discriminatory or not discriminatory at all.
- 2.18. In **Case Study A**, the social media platform and the corporate that placed the advert might seek to justify the use of the adaptive algorithm and the underlying dataset on the basis that it wanted to ensure the job advert was shown to as many suitable candidates as possible. However, on the current facts, such a defence would likely fail since the same aim could have been achieved in a non-discriminatory way by simply posting the advert in a specialist STEM publication (or on a specialist STEM website), which everyone can read regardless of sex ensuring that no discrimination occurs.
- 2.19. **Case Study A** demonstrates that the Equality Act 2010, despite having been crafted before anyone perceived the need to regulate discriminatory AI-powered technology, can be moulded to meet the modern context. The Equality Act 2010 was based on European laws to prohibit discrimination and we can see similar provisions at work in a recent Italian case in which the Labour Court in Bologna held that there was indirect discrimination in some of the working practices of Deliveroo that were driven by AI.

- 2.20. In *Filcams Cgil Bologna and others v. Deliveroo ITALIA S.R.L.*,⁵⁹ the Bologna Court had to consider an app that the Italian Deliveroo company used to decide the priority it afforded the company's riders in relation to access to jobs. The system attributed all riders to three groups, having decreasing priority by reference to scores given to them based on reliability and flexibility. However, the system treated equally all data inputs in relation to the willingness of riders to work generally, and at the busiest times. That might superficially seem reasonable but of course there could be good reasons for late cancellations or inability to work such as childcare or illness, which might well affect some persons more than others so that as a result they would not be able to obtain high priority. It was clear in this sense that the system was indirectly discriminatory on several bases, such as sex, given that women would disproportionately have caring responsibilities that might arise at short notice.

The problem of getting to know what has happened

- 2.21. **Case Study A**, however, illustrates a major weakness in the current legal framework. That is, how are women who have not seen the advert to know that they have been disadvantaged? Even if they do happen to find out that they missed the advert, perhaps having learned of a male colleague who applied for the role, how are they to know, much less demonstrate, that women were treated to their detriment by the algorithm due to their sex?
- 2.22. At present, we know (primarily because of academic research) that algorithms, especially those formed through ML, can discriminate. Indeed, **Case Study A** is based on academic research that studied the way in which ad-promoted job opportunities were targeted on Facebook. The researchers discovered that across 191 different countries a "gender neutral" job advert in the STEM fields was significantly more likely to be shown to men.⁶⁰ Other research has also

⁵⁹ See Case N. R.G. 2949/2019 *Filcams Cgil Bologna and others v. Deliveroo ITALIA S.R.L.*, judgment of Dr. Chiara Zompi, 31 December 2020, available in Italian [here](#).

⁶⁰ Lambrecht, Anja and Tucker, Catherine E., Algorithmic Bias? An Empirical Study into Apparent Gender-Based Discrimination in the Display of STEM Career Ads (March 9, 2018). See [here](#).

demonstrated that women are less likely to be shown adverts for high-paying roles in general.⁶¹

- 2.23. Yet, in the absence of academic research, how is serious discrimination such as this to be uncovered? There is no mechanism within the Equality Act 2010 that assists victims to identify breaches pre-action and they may not even know that algorithms with the potential to discriminate against them are being deployed. This is a major deficiency in the legal framework.

Case Study B: The impact of biometric data analysis to score applicants

- 2.24. Discrimination can also continue during the selection process itself even if the disadvantaged group sees the advert. This scenario is addressed in **Case Study B**, which again reveals a difficulty around knowledge albeit in the context of the duty to make reasonable adjustments for disabled people.

A company offers recruitment services to large employers. It “interviews” candidates via an online platform that analyses the candidates’ words used and other data, such as facial movements, and then provides feedback to the employer which can be used as part of their recruitment decision-making process. This scoring process is informed by ML algorithms that profile candidates. One employer decides to use this online recruitment tool in order to hire a team of people on fixed-term contracts to assist with a large data entry task. A disabled man applies for one of the roles and scores poorly in the online assessment. He does not know why he has scored so poorly, although his disability does impact on his facial movements and voice, and he is suspicious that he may have been wrongly marked down for this reason. He believes that he should have been offered an in-person interview rather than being scored by an algorithm and that his score would have been more accurate if this had happened.

- 2.25. The disabled job candidate in **Case Study B** may well be right to suspect that his disability has led to an unfairly depressed mark. Research by New York’s

⁶¹ Tschantz, M.C. and Datta, A., 2015. [Automated experiments on ad privacy settings: A tale of opacity, choice, and discrimination](#). *Proceedings on privacy enhancing technologies*, 2015(1), pp.92-112.

AI Now Institute into [HireVue](#), a company that operates in the UK as well as the US and which uses biometric information to determine who would be an “ideal” employee, has been heavily criticised as discriminating against disabled individuals.⁶²

2.26. Scholars at New York’s AI Now Institute wrote in November 2019:⁶³

The example of the AI company HireVue is instructive. The company sells AI video-interviewing systems to large firms, marketing these systems as capable of determining which job candidates will be successful workers, and which won’t, based on a remote video interview. HireVue uses AI to analyze these videos, examining speech patterns, tone of voice, facial movements, and other indicators. Based on these factors, in combination with other assessments, the system makes recommendations about who should be scheduled for a follow-up interview, and who should not get the job. In a Report examining HireVue and similar tools, authors Jim Fruchterman and Joan Mellea are blunt about the way in which HireVue centers on non-disabled people as the “norm,” and the implications for disabled people: “[HireVue’s] method massively discriminates against many people with disabilities that significantly affect facial expression and voice: disabilities such as deafness, blindness, speech disorders, and surviving a stroke.

2.27. Accordingly, the disabled job candidate might have a legitimate claim against the hypothetical recruitment company, or the potential employer, if it is right that his disability has placed him at a disadvantage within the scoring process.

2.28. The duty to make reasonable adjustments is contained in [section 20 Equality Act 2010](#) as follows:

⁶² See also Kelly-Lyth, A., 2020. Challenging Biased Hiring Algorithms. *Oxford Journal of Legal Studies* [Forthcoming].

⁶³ Whittaker, M., Alper, M., Bennett, C.L., Hendren, S., Kaziunas, L., Mills, M., Morris, M.R., Rankin, J., Rogers, E., Salas, M. and West, S.M., 2019. [Disability, Bias, and AI](#).

- (1) Where this Act imposes a duty to make reasonable adjustments on a person, this section, sections 21 and 22 and the applicable Schedule apply; and for those purposes, a person on whom the duty is imposed is referred to as A.
- (2) The duty comprises the following three requirements.
- (3) The first requirement is a requirement, where a provision, criterion or practice of A's puts a disabled person at a substantial disadvantage in relation to a relevant matter in comparison with persons who are not disabled, to take such steps as it is reasonable to have to take to avoid the disadvantage.

- 2.29. Like **Case Study A**, the algorithm and even possibly the dataset at the heart of the AI and ML discussed in **Case Study B** would be a PCP or two PCPs within the meaning of section 20(3) Equality Act 2010. In so far as these PCPs put the disabled candidate at a “*substantial disadvantage*” in relation to the interviewing process, there would be an obligation to take “*reasonable*” steps to remove that disadvantage, such as conducting the interview with a human trained in equality opportunities best practice either face to face or via remote means, rather than via an algorithm.
- 2.30. The difficulty again is knowledge. How is the disabled applicant to show that which he suspects, namely that his disability has led to an unfairly depressed mark in the scoring process in comparison to non-disabled peers?

General conclusions about the Equality Act 2010

- 2.31. We can now reach our first significant conclusion.

Conclusion 1: AI, ADM and profiling can discriminate. The existing legal framework giving effect to the principle of non-discrimination in the workplace is, in principle, capable of tackling discriminatory uses of AI and ADM, but can only be used effectively where transparency is guaranteed.

- 2.32. There is a further point here. It is obvious that the AI system an employer uses will be the product of many different actors: those who wrote the initial code for the first algorithm, those who wrote the machine-learning instructions, those who supplied the initial data on which the system was trained, and so on, down to those who determined that the system should be bought and used and those who then applied its outcomes. So, we can see that discrimination might be perpetrated by an employer in circumstances where a different organisation had created the discrimination in the first place.
- 2.33. This can very simply be illustrated by examining online advertising platforms. Companies such as Twitter permit employers to target job adverts based on protected characteristics. Whilst these organisations provide the “tools” or means by which discrimination can occur, it is ultimately the employer, or an agent of the employer such as a recruitment intermediary, that will decide to target advertisements in a way that might contravene the Equality Act 2010.⁶⁴
- 2.34. Further, more complex AI systems might harvest training data from a variety of sources, which is then analysed by an algorithm created and controlled by a different actor and then finally utilised by a different organisation again. Where multiple actors play important roles in the development and use of algorithms, how is liability to be attributed? The potential problem is further exacerbated by the “black box” challenge addressed above in that opacity within an AI system may further obscure which organisation has introduced or contributed to any discriminatory features.
- 2.35. This leads us to our second conclusion.

Conclusion 2: There are difficulties with identifying when and how and by whom discrimination is introduced within the “value chain” of actors who have created an AI tool, which in turn can make it difficult for workers and employees to enforce rights to non-discrimination.

⁶⁴ There are some provisions in ss. 110–112 of the Equality Act 2010 which might help here. The principal issue is to identify where liability lies and to make sure that there is an effective mechanism.

B: Principles of observability and transparency

- 2.36. In this subsection we pick up on the points already made about knowledge, both because of the problem that discrimination can occur when AI systems operate in ways that potential employees are not even aware of, and also because, even where they are aware, they do not understand how they came to be affected.
- 2.37. The *Worker Experience Report* has highlighted particularly the second point, that there is a lack of transparency in relation to the use of AI-powered technologies generally. It stated:⁶⁵

A very common theme in both of our surveys was that workers and union reps felt there was a strong possibility that AI-powered technologies were being used in their workplace, but that they were simply unaware of this.

Unless workers are asked for their consent before AI systems are introduced at work, they may not know about an AI system being used.

Even if workers are aware of the AI system in place, they might not have a complete picture of how the system is being used. For example, lecturers might be aware of an AI-powered platform used for teaching and monitoring pupil performance, but not know whether this system performance-monitors them as well.

“The black box”

- 2.38. Concerns about a lack of transparency are not simply directed to whether an AI-powered technology is being used and, if so, when. They also relate to the inner workings of the algorithm, known colloquially as the “black box” problem. The problem was put eloquently by one legal expert, Dr Pavel Klimov, who

⁶⁵ See the TUC’s Report, “*Technology managing people: The worker experience*”, op. cit. at pages 15 to 16.

gave evidence to the House of Commons Science and Technology Committee in 2018. He explained that when ML is deployed:⁶⁶

... humans may no longer be in control of what decision is taken and may not even know or understand why a wrong decision has been taken, because we are losing sight of the transparency of the process from the beginning to the end.

- 2.39. We can explore further what the “*black box*” means in practice by returning to **Case Studies A and B**.
- 2.40. There are limited means by which the hypothetical claimants could prove a breach of the Equality Act 2010 in **Case Studies A and B**. At present, their main options would be to start by trying to:
- Identify relevant academic research, such as the work produced by the AI Now Institute, which might support their suspicions.
 - Identify other litigation, perhaps in different jurisdictions, where helpful information has been disclosed about the relevant algorithm or AI-powered technology.
- 2.41. There are a few other possibilities. A determined and well-resourced claimant might perhaps be able to identify discriminatory practices by collating data on the outputs of an AI system without needing to resort to disclosure. For example, in **Case Study A**, the claimant might be able to survey members of a specialist STEM organisation to understand how many people saw the advert so as to identify any sex-based patterns. However, it should not be underestimated how difficult a process this would be.
- 2.42. Alternatively, in recent times there has been an increased focus on organisations co-ordinating the sharing of data with a view to identifying

⁶⁶ The House of Commons Science and Technology Committee’s Report [“Algorithms in decision-making”](#), Fourth Report of Session 2017-19, on 23 May 2018, paragraph 57.

discrimination. For example, AlgorithmWatch, a European organisation, recently started a campaign to gather data about Instagram with a view to understanding how its algorithm works.⁶⁷ Similarly, grass roots activism is becoming popular as a means of understanding and challenging AI systems.⁶⁸

- 2.43. Accordingly, a mechanism for sharing data might prove a better route for the claimants in **Case Studies A and B**. We will return to this last idea in Chapter 3 within our recommendations.

Using the UK GDPR to find out what happened

- 2.44. Individuals *might* also identify discrimination through a request for information or an explanation as to the algorithm pursuant to the UK GDPR in so far as personal data is being processed.
- 2.45. The key requirements under the UK GDPR are as follows:⁶⁹
- 2.45.1. Where there is an obligation to provide information to data subjects under the UK GDPR about how their personal data is processed, it must be “*concise, transparent, intelligible*” and in an “*easily accessible form, using clear and plain language*” (Article 12).
- 2.45.2. Where personal data is collected from the data subject, there is a requirement to provide basic information such as the purposes for which the data processing will happen and the legal basis for the processing (Article 13).
- 2.45.3. Where personal data is collected from a source other than the data subject, there is a requirement to provide basic information, such as the purposes for which

⁶⁷ “[Help us to unveil the secrets of Instagram](#)” is a campaign run by Algorithm Watch which relies on data sharing to understand how an algorithm works.

⁶⁸ “[The Algorithmic Ecology: An Abolitionist Tool for Organizing Against Algorithms](#)” is an activist project aimed at challenging algorithms.

⁶⁹ Note that these obligations are disapplied by the DPA 2018 in certain situations as set out in Schedule 2, for example, where the data processing is to secure health and safety at work.

the data processing will happen and the legal basis for the processing (Article 14).

2.45.4. Data subjects also have a right to obtain a copy of the personal data that is processed through a “data subject access request” (Article 15).

2.46. Yet, for an individual in **Case Study A** or **Case Study B** to truly understand what is happening to their data and the impact it has on them, *they will need an explanation of how the algorithm is working*. Here, the UK GDPR is inadequate.

2.47. There is a requirement within the UK GDPR in Articles 13(2)(f), 14(2)(g) and 15(1)(h) to provide information to data subjects about “*the existence of automated decision-making, including profiling*” **but** there is an obligation to provide “*meaningful information about the logic involved, as well as the envisaged consequences of such processing for the data subject*” **only** where the decision-making falls into Article 22.

Article 22

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.
2. Paragraph 1 shall not apply if the decision:
 - is necessary for entering into, or performance of, a contract between the data subject and a data controller;
 - is authorised or authorised by domestic law which also lays down suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests; or
 - is based on the data subject’s explicit consent.
3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

3A. Section 14 of the 2018 Act, and regulations under that section, make provision to safeguard data subject's rights, freedoms and legitimate interests in cases that fall within point (b) of paragraph 2 (but not within point (a) or (c) of that paragraph).

4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in [Article 9\(1\)](#), unless point (a) or (g) of [Article 9\(2\)](#) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

- 2.48. As is plain from the text of Article 22, it is heavily qualified such that the obligation to provide "*meaningful information about the logic involved*" does not arise where, for example, there is human involvement in the decision-making (i.e., it is not automated) or the processing is necessary for the performance of the employment contract.⁷⁰
- 2.49. In our view, this *qualified* right to meaningful information in the context of the employment relationship is inadequate where there is a risk, for example, of discrimination arising from processing.
- 2.50. Moreover, there is nothing in the UK GDPR that requires a *personalised* as opposed to generic description of the logic which is to be provided. This point is illustrated by examining the guidance from the European Data Protection Board in relation to the EU GDPR (which is currently very similar to Article 21 in the UK GDPR) and the obligation to provide a description of "*the logic involved*" in relation to Article 22 automated processing.⁷¹ The guidance starts by stating that "[t]he GDPR requires the controller to provide meaningful information about the logic involved, not necessarily a complex explanation of the algorithms used or disclosure of the full algorithm", and then moves on to provide the following example of how this obligation can be met:

⁷⁰ Note that [Section 14\(4\) Data Protection Act 2018](#) supplements the UK GDPR and explains that data subjects must be informed as soon as reasonably practicable that a decision has been taken on the basis of fully automated processing and the data subject may then ask for a human-based review.

⁷¹ [Article 20 Data Protection Working Party Report "Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679"](#).

Example A controller uses credit scoring to assess and reject an individual's loan application. The score may have been provided by a credit reference agency or calculated directly based on information held by the controller. Regardless of the source (and information on the source must be provided to the data subject under Article 14 (2) (f) where the personal data have not been obtained from the data subject), if the controller is reliant upon this score it must be able to explain it and the rationale, to the data subject. The controller explains that this process helps them make fair and responsible lending decisions. It provides details of the main characteristics considered in reaching the decision, the source of this information and the relevance. This may include, for example:

- the information provided by the data subject on the application form;
- information about previous account conduct, including any payment arrears; and
- official public records information such as fraud record information and insolvency records.

The controller also includes information to advise the data subject that the credit scoring methods used are regularly tested to ensure they remain fair, effective and unbiased. The controller provides contact details for the data subject to request that any declined decision is reconsidered, in line with the provisions of Article 22(3).

- 2.51. It can readily be seen that this type of “*high level*” generic description of the logic used by an algorithm in a work setting – which might drive crucial decisions such as whether someone is disciplined or dismissed – is simply inadequate. It is clear that employees could lose their jobs, be disciplined or have pay determined by reference to decisions that they can never really understand.
- 2.52. Others have been considering the importance of this issue in the context of some of the most precarious working contexts. Leïla Chaibi, a Member of the European Parliament, has proposed a draft Directive to protect those in the gig economy such as bicycle couriers, VTC drivers and taxi drivers. These workers are usually recruited on a self-employed basis by digital platforms, which impose extremely onerous working conditions that are enforced by ADM with

minimal or no human intervention. One provision of her draft Directive,⁷² which could provide a model for reform in the UK, states:

1. It shall be the responsibility of platforms to make the workings of their algorithms intelligible for workers and their representatives.
2. Platforms shall indicate the main parameters which, either individually or collectively, are the most important for determining the allocation of teams, the distribution of job offers and places of work, the assessment of work carried out, the arrangements for waiting time and for determining remuneration, as well as the relative importance of these main parameters, by providing a description which is easily and publicly accessible and set out in clear and comprehensible language. Platforms shall keep this description up to date.

Opening the “black box” through litigation

- 2.53. In the absence of being able to demonstrate discrimination using the methods summarised from paragraph 2.40 above, claimants will be forced to start litigation in the hope that useful evidence is provided during the usual disclosure process.
- 2.54. Alternatively, they will have to rely on the Employment Tribunal being prepared to infer discrimination from the lack of transparency within the AI-powered process itself. The principle that a lack of transparency can give rise to an *inference* of discrimination was first laid down some thirty years ago in Case C-109/88 *Danfoss*, albeit in the context of discriminatory pay practices.⁷³ This case has been relied on in UK case law and currently remains part of the

⁷² Her proposal for a Directive of the European Parliament and of the Council On Digital Platform Workers can be accessed [here](#).

⁷³ In [Case C-109/88 Danfoss](#) the European Court of Justice held that discrimination can be inferred in some situations where there is a lack of transparency. This principle has been applied in many cases subsequently. However see also [Case C-415/10 Meister](#) in which the CJEU held that there was no right to have disclosure of unexplained material in such cases, though inferences of discrimination might otherwise be drawn.

UK's legal system post Brexit. This means that, paradoxically, the lack of meaningful transparency as to the way in which an algorithm or AI or ML model works, might *assist* claimants who are prepared to litigate without having certain evidence of discrimination.

Conclusion about the UK GDPR

- 2.55. However, it should be plain that expecting or compelling claimants to litigate discrimination claims in the absence of meaningful levels of transparency is far from ideal in that the evidential uncertainty involved in such a strategy poses risks and will likely dissuade many claimants from litigating in the first place. This leads to our third major conclusion.

Conclusion 3: The existing legal framework does not adequately compel transparency and observability around the use of AI and ADM. There is no universal legal right of “*explainability*”, and no recognised entitlement to a personalised explanation. This is problematic as applications of AI, ML and ADM in the workplace can have significant legal implications for people such as the risk of discrimination.

International trade in intellectual property rights

- 2.56. Much work is done outside the UK to set up AI systems, develop algorithms and create ML and ADM. Even where these systems are set up within the UK, it is likely to be subject to great secrecy to preserve intellectual property rights (IPR).⁷⁴ Nobody doubts that the creation of IPR provides an economic incentive for useful and imaginative creativity. They are not inherently bad, and it is only to be expected that their owners will seek to protect their value by imposing confidentiality on those to whom they sell or licence these rights.

⁷⁴ A European Commission literature review published in 2019 noted that the software and data that creates AI may be protected by copyright or as trade secrets. It concluded that insufficient attention has been paid to the tension between the need for explainability and transparency as against intellectual property rights. The European Commission's “Intellectual Property and Artificial Intelligence – A literature review” is available [here](#). Others including Lord Sales, a member of the UK's Supreme Court, have suggested that a specialist court might be necessary to review and monitor AI, possibly with rules that limit the extent to which sensitive commercial data could be shared publicly.

- 2.57. Yet, these intellectual property rights cannot be permitted to impede the right to enforceable protection from discrimination by undermining the transparency and explainability required by equality law to ensure that AI is used lawfully and ethically. This is a special problem in international trade agreements, which often have clauses that seek to protect confidentiality in IPRs when traded across borders. For instance, the [UK-Japan Comprehensive Economic Partnership Agreement of the 23 October 2020](#) (the UK-Japan CEPA)⁷⁵ states in Article 8.73:⁷⁶

Source code

1. A Party shall not require the transfer of, or access to, source code of software owned by a person of the other Party, or the transfer of, or access to, an algorithm expressed in that source code, as a condition for the import, distribution, sale or use of that software, or of products containing that software, in its territory.
2. This Article shall not preclude a regulatory body or judicial authority of a Party, or a Party with respect to a conformity assessment body, from requiring a person of the other Party: (a) to preserve and make available the source code of software, or an algorithm expressed in that source code, for an investigation, inspection, examination, enforcement action or judicial proceeding, subject to safeguards against unauthorised disclosure; or (b) to transfer or provide access to the source code of software, or an algorithm expressed in that source code, for the purpose of imposing or enforcing a remedy granted in accordance with that Party's law following an investigation, inspection, examination, enforcement action or judicial proceedings.
3. This Article does not apply to: (a) the voluntary transfer of, or granting of access to, source code, or an algorithm expressed in that source code, by a person of the other Party, such as in the context of a freely negotiated contract or government procurement; or (b) services supplied or activities performed in the exercise of governmental authority.

⁷⁵ CS Japan No.1/2020, CP 311 Volume 1, see [here](#).

⁷⁶ The Article proceeds with some exceptions, but none appears to relate to the kind of problem that this Report concerns. Footnotes omitted.

- 2.58. In the context of UK trade policy post Brexit, it is significant that the UK “explainer” of the “[Digital and Data provisions in the UK-Japan CEPA](#)” explains how this agreement goes further than the existing EU-Japan agreement:

The UK and Japan have also expanded on important areas within [the EU-Japan \[Economic Partnership Agreement\]](#).^[77] In particular, the agreement prevents the forced transfer of algorithms, broadens digital trade facilitation, for example through encouraging the use of interoperable electronic authentication and electronic signatures, and expands future cooperation in various areas, including emerging technologies and electronic trust services.

- 2.59. The European Parliament had earlier addressed this kind of issue on 2 September 2020 stating:

AI makes it possible to process a large quantity of data relating to the state of the art or the existence of IPRs [Intellectual Property Rights]; [Parliament] notes, at the same time, that AI or related technologies used for the registration procedure to grant IPRs and for the determination of liability for infringements of IPRs cannot be a substitute for human review carried out on a case-by-case basis, in order to ensure the quality and fairness of decisions; [Parliament] notes that AI is progressively gaining the ability to perform tasks typically carried out by humans and stresses, therefore, the need to establish adequate safeguards, including design systems with human-in-the-loop control and review processes, transparency, accountability and verification of AI decision-making...⁷⁸

⁷⁷ The EU-Japan Economic Partnership Agreement entered into force on 1 February 2019.

⁷⁸ The European Parliament's view on the interplay between AI and intellectual property rights can be accessed [here](#).

- 2.60. It is obvious that free trade agreements can have strong beneficial economic effects, nonetheless these kinds of agreements have given rise to concerns about the protection of IP from transparency.⁷⁹ As a result of such concerns, in October 2020 the European Parliament recommended that the European Commission conduct an impact assessment on the implications of AI and related technologies under the current system of patent law, trademark and design protection, copyright and related rights, including the legal protection of databases and computer programs, and "*trade secrets*", concluding that EU laws must be amended as necessary. It urged the Commission to support standardisation in the development and dissemination of new AI and related technologies, and to create a balanced European data space to foster the free flow, access, use and sharing of data, while protecting IPRs and trade secrets.⁸⁰
- 2.61. The ETUC and the ITUC have raised similar issues, highlighting, amongst other matters, the importance of social partners being involved in decisions about how intellectual property rights are protected.⁸¹ This is an important and pressing issue because across the world there is a trend to enter into so-called "*Digital Economy Agreements*". Examples include the Australia-Singapore Agreement⁸² and the New Zealand, Chile and Singapore Agreement.⁸³ The UK has specifically praised the Australia-Singapore Digital Economy Agreement as being innovative and a model for an agreement between Australia and the UK.⁸⁴

⁷⁹ See for instance the submission by the Australian Council of Trade Unions to the Australian Joint Standing Committee on Treaties accessible [here](#).

⁸⁰ See [here](#).

⁸¹ The ETUC position on ecommerce negotiations is available [here](#). The ITUC Report 'Free Trade Agreements, Digital Chapters and the impact on Labour' is available [here](#). Many of trade unions' concerns about digital chapters in trade negotiations are flagged in a recent Report by trade justice campaigner Deborah James, *Digital Trade Rules: A Disastrous New Constitution for the Global Economy Written By and for Big Tech*, published by the Centre for Economic and Policy Research and available [here](#).

⁸² This can be accessed [here](#).

⁸³ This can be accessed [here](#).

⁸⁴ See [here](#).

Conclusion about trade in IPRs

- 2.62. To our knowledge nothing equivalent to the European Parliament proposal, referred to in paragraph 2.60 above, has been proposed for the United Kingdom so concerns remain that new international trade agreements between the UK and other countries with clauses such as those noted in the UK-Japan CEPA could be read as conferring a secrecy on IPR that would be inconsistent with the proper regulation of their use within the UK. Of course, the UK operates a dual system of law in that trade agreements are made under the prerogative and do not form part of domestic law unless and until they have been brought within domestic legislation. So, the scrutiny of the effect of such trade agreements will be critical so that transparency and its important role in ensuring equality is promoted.
- 2.63. The fear is that Brexit could make such proposals even more necessary. One justification for Brexit was that it liberated the UK to enter into its own trade agreements. The fear is that the dynamic created by Brexit towards a raft of speedy agreements could undermine existing protections and make it harder to improve on them.
- 2.64. It is easy to think of examples where this could be very significant as, for instance, the use of recruitment systems provided by HireVue, which use ML to make recommendations for both hiring and firing. If employees are unable, because of international rules on IPR secrecy, to get a full understanding of what has happened to them, that would be wholly inconsistent with equality principles and standard AI ethics.
- 2.65. So, while we acknowledge that international trade agreements are important, they are not so important as to undermine the principle of equal treatment; this leads us to our fourth conclusion.

Conclusion 4: Intellectual property rights, and their protection under international trade agreements, have the potential to impede the degree of transparency necessary to ensure the lawful and ethical use of AI and ADM. This must not be allowed to happen as it will make an existing difficulty in holding AI systems to account even more difficult.

C: Right to privacy

- 2.66. The increased use of technology has also enabled employers to monitor their workforce in new ways, leading to concerns that the “*private space*” of employees and workers is being eroded. Thus, the *Worker Experience Report* found that 27% of workers surveyed had their communication screened, 13% had experienced desktop monitoring and 8% were aware of social media screening.⁸⁵ The Report also highlights evidence that this surveillance has increased in light of the pandemic and homeworking.
- 2.67. This trend is exemplified in the case study below, which has been formulating using real-life experiences captured by the TUC in its Report.

Case Study C: Monitoring productivity

A large employer uses an online tool which allocates tasks to employees, imposes deadlines, tracks when a piece of work has been completed and monitors when people are “*available/away/offline*” and when they were “*last active*”. During the pandemic when staff members were compelled to work from home, this online monitoring continued. The tool was used to log the hours worked by staff, the number of keyboard strikes made in an hour, social media was recorded, and photographic “*timecards*” were taken every 10 minutes via a webcam.

- 2.68. **Case Study C** directly engages the HRA, which incorporates the ECHR into domestic law. It remains part of the UK legal system and is unaffected by Brexit. As a starting point, it is worth noting that the ECHR is a “*living instrument*”, meaning its provisions must be interpreted in light of changing standards in the field of human rights and technological and scientific developments so that its protections remain practical and effective.⁸⁶ Accordingly, we expect Article

⁸⁵ See the TUC’s Report, “*Technology managing people: The worker experience*”, op. cit. supra at page 27.

⁸⁶ See *Tyrer v United Kingdom* (App No. 5856/72, 25 April 1978).

8 (set out above at paragraph 1.52) to be moulded to meet new AI-powered technologies.

- 2.69. It is likely that the type of intrusive processing of employee personal data in **Case Study C**, whilst employees are compelled to work at home, for the purposes of productivity monitoring will fall within the scope of Article 8.⁸⁷ It is also likely that the video surveillance and the accessing of personal data constitutes an interference with employees' privacy rights under Article 8.⁸⁸ The compatibility of the monitoring in **Case Study C** with Article 8 therefore turns on whether the inference can be justified under Article 8(2).
- 2.70. There are three steps that must be taken to establish a successful justification under Article 8(2).
- 2.70.1. First, the interference must be in accordance with law. Here, on the assumption that the monitoring is compatible with the UK GDPR and the DPA, which is further explored below, it will be in accordance with the law.⁸⁹
- 2.70.2. Second, the interference must pursue a legitimate aim. It is well-established that employers have '*a legitimate interest in ensuring the smooth running of the company, and that this can be done by establishing mechanisms for checking that its*

⁸⁷ The ECHR has yet to adjudicate on whether processing employee personal data, whilst they are home, for the purposes of productivity monitoring will fall within the scope of Article 8. However, it is well-established that privacy protections under Article 8 extend to one's professional activities and employment (see [Barbulescu v Romania](#) (App No. 61496/02, 2 September 2017 (GC)). In principle, it is therefore clear that the fact that employees are engaging in work when being monitored at home does *not exclude* the protection of their privacy under Article 8. Whether privacy protections under Article 8 ultimately apply in the context of work often rests on whether employees have a '*reasonable expectation that their privacy would be respected and protected*' (see [Barbulescu](#)). In **Case Study C**, the breadth of the monitoring and the fact the employees are based at home by necessity supports the view that they have a reasonable expectation of privacy. Whilst this expectation may be reduced during the hours of work and if the employer has given advance notice that they will be monitored, the better view is that Article 8 is engaged but that these factors are relevant to the proportionality assessment but do not exclude one's rights to privacy under Article 8 to zero (see [Barbulescu](#)). It is therefore likely that **Case Study C** falls within the scope of Article 8.

⁸⁸ See [Antovic and Mirkovic v Monetenegro](#) (App No. 70838/13, 28 November 2017); [Amann v Switzerland](#) (App No. 27798/95, 16 February 2000).

⁸⁹ See [Copland v United Kingdom](#) (App No. 62617/00, 3 April 2007).

*employees are performing their professional duties adequately’.*⁹⁰ The monitoring in **Case Study C** therefore likely pursues a legitimate aim.

2.70.3. Third, the interference must be necessary in a democratic society. That is, it must correspond with a pressing social need and is proportionate to the legitimate aim pursued. The following factors will be relevant in determining whether the monitoring of employees in **Case Study C** is proportionate to this interest:

- Whether the employer notified the employees of the nature and scope of the monitoring;
 - The extent of the intrusion into the employees’ privacy;
 - Whether the employer has provided legitimate reasons for the monitoring;
 - Whether a less intrusive form of monitoring could have been used;
 - The effectiveness of the monitoring in ensuring the smooth running of the employer’s business;
 - The consequences of the monitoring on the employees;
 - Whether there were adequate safeguards in place;
- and
- Whether the monitored employee is in a regulated profession, such as social services, where, due to the sensitivity of the work involved and stronger public interest for employee accountability, monitoring may well be more readily justifiable.

2.71. Accordingly, this stage of the justification defence requires a detailed examination of the facts before any final decision as to whether Article 8 has

⁹⁰ See [Barbulescu](#).

been breached can be made. It follows that whether a violation can be established will be highly fact sensitive.

- 2.72. There is a particular issue about Article 8 rights that must be noted. The ECHR gives these rights to individuals vis-à-vis the state. It is the state's obligation to ensure that they are protected. That means that the deployment of these rights in disputes with private employers can be complicated. There are various means by which this can be done including through the interpretative provisions in section 3 of the HRA and the obligations on courts to respect these rights in section 6. Courts and tribunals have developed some experience of ensuring such rights since the HRA was passed. Nonetheless, the fact that they are written in terms that impose obligations on the state rather than directly on the employer does make for some difficulties.

Conclusion about the right to privacy

- 2.73. Our concern is that at present there is inadequate legally binding guidance to employers explaining when Article 8 rights are infringed by the use of AI-powered technology and how, practically speaking, the Article 8 balancing exercise is to be resolved. In the light of the great increases in workplace surveillance, especially at a time of pandemic and increased home working, this is deeply unsatisfactory. Employers, trade unions, employees and workers should be able to assess reliably whether an AI-powered tool is compatible with Article 8. They should not be compelled to litigate in order to demonstrate non-compliance. This leads to our fifth conclusion.

Conclusion 5: Article 8 ECHR is adequate to protect the privacy of employees and workers from intrusive forms of AI and ADM. However, at present there is inadequate legally binding guidance to employers explaining when Article 8 rights are infringed by the use of AI-powered technology and how, practically speaking the Article 8 balancing exercise is to be resolved. Without such guidance employers will not fully understand their obligations, nor will employees be able to hold the line against inappropriate incursions into their right to a private life.

D: Right to data protection

- 2.74. Workers and employees also have a fundamental right to the protection of their data rights.
- 2.75. We identified in paragraph 2.70.1 above that the monitoring in **Case Study C** would be lawful, and therefore compatible with Article 8, only in so far as it was consistent with the UK GDPR and DPA. We now turn to consider how **Case Study C** would be analysed within the data protection framework in the UK.
- 2.76. The first point to make is that the monitoring in **Case Study C** would fall squarely into the UK GDPR since:
- Information regarding an employees' hours, keyboard strikes, and social media use, and their photographic timecards, would fall within the wide definition of "*personal data*" under Article 4(1);⁹¹
 - The collection of the information through the online tool amounts to "*processing*" of data under Article 4(2); and
 - The analysis of work performance to determine productivity will likely amount to a form of processing known as "*profiling*" under Article 4(4); a concept we first introduced in paragraph 1.14 above.

⁹¹ For the purposes of **Case Study C**, we have assumed that the data is not special category data. It is theoretically possible that the photographic timecard data is also biometric data under Article 9 and accordingly "*special category data*", which is subject to more stringent legal rules. There is a common view of Article 9 is that it only covers biometric data which is used to identify *who* someone is rather than the *type of person* that they are. We stress that point here because from an employment law perspective there are real concerns about AI being used to make judgements about what type of person an employee is, e.g. lazy, fraudulent, hardworking. It seems to us that there may be powerful arguments that biometric data within Article 9 should accordingly cover data which is used to categorise the type of person someone is rather than simply who they are. Such a change would, of course, have wide ranging implications beyond the employment sphere since the UK GDPR applies to all data processing subject to certain specific exceptions. We are aware that Matthew Ryder QC is currently carrying out a review of biometric data on behalf of the Ada Lovelace Institute and believe that this issue will be addressed further in his report.

- 2.77. The result is that the employees in **Case Study C** are “*data subjects*” who have enforceable rights in relation to how this data is collected and used; and the employer is a “*data controller*” who must comply with their UK GDPR and DPA obligations when using the online tool.
- 2.78. This means that the employer must process any employee data gathered by the online tool lawfully, fairly and in a transparent manner (Article 5). Specifically, the processing of the data will be unlawful unless one of the following (relevant) conditions is satisfied:
- The employees consented to the processing of their data (Article 6(1)(a));
 - The data processing is necessary for the performance of the employment contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (Article 6(1)(b)); and
 - The data processing is necessary for the purposes of a legitimate interest, provided this is not overridden by the fundamental rights of the employee (Article 6(1)(f)).
- 2.79. In lieu of employee consent which, even if given, will often be unlikely to be true consent given the power imbalance in the employment relationship, it would be open for the employer in **Case Study C** to argue that the processing of data is necessary to ensure that employees perform their obligations under their employment contract (Article 6(1)(b)) or alternatively that the data processing is necessary for the purpose of its legitimate economic interest to maintain workforce productivity (Article 6(1)(f)). This exception will thus often undermine what seems at first glance to be a very important protection for the employee.

Conclusions about data protection

- 2.80. Here, we encounter problems with the legal framework as it currently stands. The logic of Article 6(1)(b) is that potentially a very wide range of data

processing will be lawful simply by virtue of the AI-powered technology being used in the context of the employment relationship and there is, accordingly, a risk that data processing becomes *de facto* lawful.

- 2.81. Whilst there is an important safeguard within Article 6(1)(b), namely that the processing must be “*necessary*” for the purposes of the employment contract, there has been minimal case law on what this means⁹² and there is no employer-focused legally binding guidance.
- 2.82. Since Article 6(1)(b) is likely to be an important “*gate keeper*” provision that will define the scope of lawful processing in the context of the employment relationship, in our view it urgently requires clarification. The need for clarity is particularly pressing since it can be immediately seen from **Case Study C** that what amounts to “*necessary*” processing is far from plain. Whilst the logging of employee hours and social media use could theoretically be considered necessary to ensure employees have worked their contractual hours, the situation in relation to photographic timecards taken every 10 minutes appears far less “*necessary*” for this purpose and may well be unlawful.
- 2.83. Such uncertainty undermines workers’ rights and has to be addressed; so, our sixth conclusion is as follows.

Conclusion 6: The data protection framework contained in the UK GDPR and the DPA 2018 has the potential to provide valuable protection to workers and employees in that data can be processed only on certain specified grounds. However, one lawful basis for data processing by an employer is that it is “*necessary*” for the performance of the employment contract (UK GDPR, Article 6(1)(b)). Unless this ground is carefully defined, which at present it is not, there is a substantial risk that all data processing within the employment relationship will be treated as consistent with the UK GDPR.

⁹² For example, [Hopkins v Commissioners for her Majesty's Revenue and Customs](#) [2020] EWHC 2355 (QB).

- 2.84. Article 6(1)(f) poses similar difficulties. It permits employers to process data even if it is not necessary for the employment contract provided that the processing is “*necessary*” to cover its legitimate interests or that of a third party. Again, there is minimal case law and no legally binding guidance on what processing would fall into Article 6(1)(f) in the context of the employment relationship, but which would otherwise not fall into Article 6(1)(b). Again, it is readily apparent that, interpreted too liberally, an employer would nearly always be able to find a lawful basis for data processing on the basis that it is pursuing its own interests.

Conclusion 7: A further lawful basis for data processing is that it is necessary for the purposes of a legitimate interest, provided this is not overridden by the fundamental rights of the employee (UK GDPR, Article 6(1)(f)). Unless this ground is carefully defined, which at present it is not, there is a risk that all data processing within the employment relationship will be treated as consistent with the UK GDPR.

- 2.85. The extent to which the employer can act lawfully under Article 6(1)(b) or (f) is also highly relevant to the important rights under Articles 22 and 21(1) of the UK GDPR, which prohibit fully automated decision-making and creates a right to object to data processing including profiling. Specifically, Articles 22 and 21 are engaged if the processing is undertaken lawfully pursuant to Article 6(1)(f) but not if it is under Article 6(1)(b).

Article 21

1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. ²The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

- 2.86. Article 22 is already outlined above at paragraph 2.47 above.
- 2.87. In other words, identification of the correct lawful basis under Article 6 defines the scope of workers' rights more broadly under the GDPR. This makes the lack of clarity as to when Article 6(1)(f) applies as opposed to Article 6(1)(b) a very serious failing.

Conclusion 8: The data protection framework contained in the UK GDPR has the potential to provide valuable protection to workers and employees in that, dependent on the lawful basis for the processing, there is a right not to be subject to fully automated decision-making (Article 22) and a right to object (Article 21). However, since the lawful basis of data processing under Article 6 dictates the availability of these rights, the lack of clarity around Article 6 creates serious uncertainty about the scope of workers' rights.

- 2.88. Finally, it is important to note that once the correct legal basis has been identified, an employer can still override an employee's right to object to data processing under Article 21 and their right to avoid fully automated decision-making altogether under Article 22, where the various exceptions in those provisions apply. Again, there is minimal case law to assist the parties to navigate the meaning of these important rights and no legally binding guidance. Clarification of these important concepts should not be dependent on the ability of workers and employees to litigate these provisions.

Conclusion 9: The important rights in Article 21 and Article 22 of the UK GDPR are subject to various exceptions, which are insufficiently defined. The lack of clarity creates serious uncertainty about the scope of workers' rights.

E: Protection from AI-powered decisions that are irrational or unfair

- 2.89. As we have noted in [Chapter 1](#), AI-powered technologies are also being used to drive important decisions, for example to decide who should be made redundant or whether undesirable behaviour has occurred. However, technology is not perfect or beyond criticism. Ordinarily, a worker or employee can ask questions or seek to challenge a human-made decision to understand whether it is rational and fair. When AI or ADM is used, this may be much harder.
- 2.90. Indeed, the *Worker Experience Report* has highlighted concerns around the ability of employees and their representatives to challenge managers when they use technology. It noted that:⁹³

The experience of trade union representatives is that often managers do not understand how AI-powered technologies work, and that this inhibits communication and the ability to challenge decisions.

Our trade union reps survey revealed these observations about employers from reps encountering difficulties with challenging AI decisions:

- management refusing to listen and believing that algorithms and technology can't be wrong
- a lack of knowledge about the algorithms used or how they work
- a lack of technical knowledge and understanding

Case Study D: The impact of flawed algorithms on workers and employees

- 2.91. Our next example, **Case Study D**, explores how errors can arise in practice following the adoption of AI-powered performance management systems.

⁹³ See the TUC's Report, "*Technology managing people: The worker experience*", op. cit. supra at page 15.

A long-standing employee had experienced a difficult period in her personal life though, thankfully, her personal circumstances had resolved, and she was maintaining an excellent attendance record. Prior to her attendance improving, she had been absent from work for many periods of time for stress-related absences.

Her employer uses an absence-management system which monitors the attendance records of all staff and will automatically trigger progressive stages of its absence management process. Equally, unauthorised absences will trigger performance management processes on the basis that it is considered a disciplinary offence. The employee was on a final written warning due to several periods of unauthorised absence, although this was about to expire due her current excellent attendance record. Unfortunately, there was an unavoidable further period of absence which was adequately explained by a GP's fit note and should have been recorded as an *authorised* absence. This fit note was not correctly processed by the automated absence management system and she was invited to a dismissal hearing. At the dismissal hearing, the relevant manager believed – because the automated system had informed her – that the employee had breached the absence management procedure. She dismissed the employee.

- 2.92. The employee in **Case Study D** would be able to bring an unfair dismissal claim assuming that she had two years' continuous service. For a dismissal to be fair under sections 97 and 98 of the Employment Rights Act 1996, it must be fair in all the circumstances, which include by reference to the procedure that has been followed and the extent to which the decision to dismiss falls within the range of reasonable responses open to a reasonable employer. The dismissal would likely be unfair because, at the very least, the conclusion that the employee had a final period of unauthorised absence is factually incorrect due to a flawed AI system and it would therefore be unreasonable to rely on that assessment.

Conclusions about the protections from irrational and unfair decisions

- 2.93. We would expect that the claimant in **Case Study D** would be able to demonstrate the factual inaccuracy giving rise to dismissal relatively easily by showing the appeals officer (or, if necessary, an Employment Tribunal) the

GP's fit note. However, as outlined identified in section 2B above, AI-powered systems are not always comprehensible so that errors can be easily identified.

- 2.94. It follows that if **Case Study D** is tweaked so that the performance management system is difficult to understand or comprehend because of the "*black box*" problem, the dismissal would also be unfair due to a lack of transparency. So, this leads to our tenth conclusion.

Conclusion 10: Unfair dismissal legislation should protect employees who qualify for protection under s.97 and s.98 of the Employment Rights Act 1996 from dismissal decisions that are factually inaccurate or opaque in the usual way. The use of AI-powered tools to support such decisions does not make any difference to this important legal protection.

- 2.95. But unfair dismissal legislation is not universal. Employees will only benefit from such protection once they have two years of service, and two years is a long time to wait for an employee to obtain vital protection against dismissal. An employee with less than two years' service without the protection of unfair dismissal legislation would likely feel extremely vulnerable and may face an employer that is not incentivised to carefully review the AI system so as to understand whether dismissal is appropriate.
- 2.96. Equally, workers have no protection from unfair dismissals at all. In these scenarios, the employee with less than two years' service, or the worker regardless of the length of their contract, would be left with protection only from the UK GDPR and in particular the requirement within Article 5(1)(d) that all personal data that is processed must be accurate. These rights – whilst valuable – cannot be sued on in the relatively cheap and accessible Employment Tribunal jurisdiction.

Conclusion 11: Alongside unfair dismissal rights for employees with two years' continuous service, there is some protection for employees and workers who are subject to decisions that have been informed by inaccurate data and /or data processing in that all personal data which is processed as part of an AI-powered technology or ADM must be accurate (Article 5(1)(d), UK GDPR). These rights could be sued on in the event of disciplinary action or other detrimental treatment arising from the use of AI. However, unfair dismissal rights are not universal, and the UK GDPR cannot be sued on in the relatively cheap and accessible Employment Tribunal, meaning that there are gaps in effective legal protection.

F: Management within a personal relationship

- 2.97. The increased reliance on technology to make management decisions risks profoundly undermining the personal nature of the employment relationship. Humans have the potential to provide an empathetic and nuanced responses within decision-making, which is currently beyond AI-powered tools.
- 2.98. The UK GPDR places some limitations on ADM where no human decision-maker is involved. We have explored these rights extensively in paragraph 2.47 onwards and commented on their qualified nature and limitations.
- 2.99. We should also highlight section 14 of the DPA, which provides a right to a human review of a decision that has been made by a fully automated decision-making process *but only where that processing is made lawful by a legal enactment*. In other words, there is no automatic right to a human review of a decision where an employer decides to process data because it is necessary by virtue of the employment contract or its legitimate interest (the distinction between these grounds for processing is explored in paragraph 2.78 above). There does not seem to us to be any good basis for making this distinction and, with the developing use of AI systems, we do not believe it can be maintained.

Conclusion about management within a personal relationship

- 2.100. The absence of an automatic obligation to provide a human decision-maker for decisions that will have significant implications for employees is a major limitation to the existing legal framework, bearing in mind the personal nature of the employment relationship. Further, the absence of a human decision-maker means that workers will be exposed where decisions, which require empathy and the “*human touch*”, are made about them by an algorithm. Where human involvement is lacking and the expectations of employees by their employers become more and more a matter of digitised targets, the role of the employee is increasingly diminished. We return to our starting point that humans are not robots and they should not be expected to act as such.
- 2.101. This leads us to the recent discussion about “*a right to analogue*” engagement. Disability and age NGOs have been arguing for a right to analogue engagement. After all, where there is no or limited access to the internet or where the engagement is particularly difficult to understand or adapt to, this may breach other rights. The fact that many older persons and persons with a disability may not be able to access the digital world on an equal footing has been a basis for arguing that there should be a right to analogue engagement where individuals are not merely reduced to data flow but are dealt with in person and as individuals.

Conclusion 12: The personal nature of the employment relationship is threatened if there is no entitlement for employees to insist that certain decisions are made about them by a human being as opposed to being fully automated. Equally, workers are exposed where decisions that require empathy and a “*human touch*” are made about them by an algorithm. Further, for some employees and workers, technology is difficult for them to access, use or understand. The failure to provide these groups with access to a human decision-maker will lead to marginalisation.

G: Protection of workers' private time from the intrusion of technology

2.102. The *Worker Experience Report* identified the toll that the increased use of AI and ADM is having on the mental health of workers. This is readily understandable as there has been a slow shift in the culture of the workplace. These new forms of technology have led people to feel pressured, requiring them to be always “on” and “available”, a matter which is discussed in more detail at paragraph 1.26 onwards.

2.103. Fears that technology has become all pervasive and started to impact on people's mental health has led to a renewed discussion about how best to protect workers and employees. Some private organisations, like Telefónica, have been proactive in signing up to agreements which recognise that employees have a right to digitally disconnect.⁹⁴ Some trade unions such as Prospect have also been actively promoting the idea, with publications such as “*Right to disconnect: A guide for union activists*”, which helpfully summarises similar approaches in jurisdictions as diverse as Germany, Argentina and New York City.⁹⁵ We are also aware of proposals around a right to disconnect being advanced by the Maltese government.⁹⁶ In the Republic of Ireland, similar proposals have been put forward by the Opposition party and appear to be under active discussion.⁹⁷

2.104. An OECD report⁹⁸ published in 2019 has noted that:

⁹⁴ More information about Telefónica's decision to recognise that its employees have a right to digitally disconnect is accessible [here](#).

⁹⁵ Similar guides have been produced by UNI Europe which are available [here](#).

⁹⁶ The Malta-EU Steering and Action Committee held a conference on this issue on the Right to Disconnect on 29 October 2019 which can be seen [here](#). The announcement of the Maltese Government's proposal to take this forward with legislation can be accessed [here](#).

⁹⁷ The Bills are the Organisation of Working Time (Amendment) (Right to Disconnect) Bill 2020 and Working from Home (Covid-19) Bill 2020. For a discussion of their implications see Crowley D., “Legal Status of the Right to Disconnect in Ireland”, see [here](#).

⁹⁸ See Cazes, S., Garnero, A., Martin, S. and Touzet, C., 2019. Collective Bargaining Systems and Worker Voice Arrangements in OECD countries. Negotiating Our Way Up, p.229 and ff., see [here](#).

In France ... the “right to disconnect”, i.e. the right not to read and answer work-related emails and calls outside working hours, was provided in 2014 in a sectoral agreement for business consulting, followed by the wholesale trade sector in 2016. These agreements introduce “an obligation to disconnect distant communication tools”. Similar provisions have been signed at firm level, for instance by the insurance company AXA, the energy company Areva and the telecommunication company Orange. The HR Director of Orange then published a very influential report on digital transformation and quality of life at work (Mettling, 2015)^[99]. The report was the basis for a law in 2017 that acknowledged the “right to disconnect” among the topics of mandatory annual negotiations with unions. In the absence of an agreement, employers have to draft a charter in consultation with the works council or the employee representatives.

2.105. The threat posed by new forms of technology was also discussed by the European Parliament in the summer of 2020. The European Parliament’s Committee on Employment and Social Affairs prepared a draft Report with recommendations to the European Commission on the development of “a right to disconnect”.¹⁰⁰ This argued that workers should have the right to be disengaged from the digital world at certain times and in some contexts. The Report identified the problem in this way:

... the advancement and impact [of] information and communication technologies (ICT) have on the world of work in many sectors and occupations, [have made] it possible for work to be taken anywhere and carried out anywhere and at any time and for workers to be reachable outside their working hours. As a result, many new challenges have evolved beyond the existing [EU’s] legal framework. The widespread use of digital tools, including ICT, for work purposes has enabled workers with greater working time autonomy and flexibility in work organisation. In contrast, however, they also have created new ways of extending working hours and diluting the boundaries between working and free time. They

⁹⁹ Mettling, B. (2015), Transformation numérique et vie au travail.

¹⁰⁰ The Report can be accessed [here](#).

have also been associated with types of “work nomadism”, as a result of which workers often become unable to disconnect from work, which, over time, leads to physical and mental health problems, such as stress, anxiety, depression and burnout, as well as impacting negatively on workers’ work-life balance. Furthermore, since the beginning of the COVID-19 crisis, flexible and remote working arrangements using digital tools, including ICT, have proved to be effective for business continuity in some industries and there has been a spike in the number of teleworkers and teleworkable solutions, which are expected to become increasingly common in the aftermath of the COVID-19 crisis.

- 2.106. At present, here in the UK, there is a detailed legal regime which requires employers to protect the health and safety of employees. However, to our knowledge this legislation has yet to be used to protect staff from the impact of new technology in relation to mental health. There are, of course, also laws concerning working time that set minimum rest breaks during the working day, minimum levels of holiday leave, and maximum working weeks (subject to any opt out). But, most importantly, there is no positive right to create “*communication free*” time in the lives of workers and employees when they cannot be contacted by management or colleagues unless there are important reasons to do so. Since we have now reached the stage as a society where technology has meant that communication has become easier and easier, we view this as a very serious deficiency in current legal protections.

Conclusion 13: The increased use of technology is encroaching more on workers’ lives, leading to a slow erosion of the distinction between work and private time due to the ease with which communication can take place. There is no existing legal tool in the UK that creates a positive right to enforce boundaries around communication during the personal life of an employee or worker, which may otherwise be eroded by technology.

H: Rights of association and bargaining

2.107. The degree to which there is a right to effective collective bargaining in the UK has been the subject of much discussion and will be well known to the TUC. Where there is no right to union recognition there is little that a union can do to force collective bargaining. Where there is recognition, then there are rights under section 181 of the Trade Union and Labour Relations (Consolidation) Act 1992 (**TULRCA**).¹⁰¹ Importantly section 181(2) states that:

- (2) The information to be disclosed is all information relating to the employer's undertaking (including information relating to use of agency workers in that undertaking) which is in his possession, or that of an associated employer, and is information –
- (a) without which the trade union representatives would be to a material extent impeded in carrying on collective bargaining with him, and
 - (b) which it would be in accordance with good industrial relations practice that he should disclose to them for the purposes of collective bargaining.

2.108. This could be very relevant in determining what use should be made of new technologies. The problem is that the right follows recognition. It is not necessary in this Report to develop these limitations. It is more important to note in some countries collective bargaining can be very effective in addressing AI systems. The OECD has noted how in some countries:

¹⁰¹ See [here](#).

... unions and employers are engaging in “algorithm negotiations”, i.e. they are including as a subject of bargaining the use of artificial intelligence, big data and electronic performance monitoring (“people analytics”) in the workplace, as well as their implications for occupational health and safety, privacy, evaluation of work performance and hiring and firing decisions (De Stefano, 2018).^[102] Several collective agreements have started regulating the use of technology not only in monitoring workers but also in directing their work (Moore, Upchurch and Whittaker, 2018).^[103]

- 2.109. The *Worker Experience Report* identified that 75% of respondees felt that there should be a legal requirement to consult staff before any new form of workplace monitoring was introduced.¹⁰⁴ Such a right would be very significant in moderating the worse effects of AI systems and in promoting trust. For these reasons we conclude that:

Conclusion 14: AI and ADM pose a significant risk to the welfare of the workforce. However, existing legislation does not mandate collective bargaining in relation to their use. Consultation and a right to collective bargaining in relation to their introduction and use is necessary to promote trust, avoid abuses and secure its beneficial use.

- 2.110. The *Worker Experience Report* also highlighted that in the US there are worrying developments in relation to using AI-powered technologies to suppress union activities such that algorithms are being used to identify (and avoid) job

¹⁰² De Stefano, V., 2019, *Negotiating the Algorithm*: Automation, Artificial Intelligence, and Labor Protection,, op cit supra.

¹⁰³ Moore, P.V., Upchurch, M. and Whittaker, X., 2018. Humans and machines at work: monitoring, surveillance and automation in contemporary capitalism. In *Humans and Machines at Work* (pp. 1-16). Palgrave Macmillan, Cham.

¹⁰⁴ See the TUC's Report, “*Technology managing people: The worker experience*”, op. cit. supra at page 41.

candidates who are likely to become trade union activists, predict worksites for the likelihood of unionisation, and suppress union-related content.¹⁰⁵

- 2.111. If an employer in the UK attempted to use AI to suppress union membership or activities of their employees and workers, there would be legal implications under TULRCA.¹⁰⁶
- 2.112. First, if an employer utilised AI software to identify candidates' union membership and activities, or to predict their likelihood of membership and activity, and this data significantly influenced a decision to refuse a person employment, this would be unlawful under section 137(1) TULRCA. The employer could not avoid liability by outsourcing the recruitment process to an employment agency or software company (section 137(8) TULRCA).
- 2.113. Second, if data gathered by AI software regarding an employee's trade union membership or activity was the principal reason for a decision to dismiss or select an employee for redundancy, it would be unlawful under sections 152 and 153 TULRCA, respectively. This protection applies regardless of an employee's length of continuous employment (section 154 TULRCA).
- 2.114. Workers are not covered by the above protections.¹⁰⁷ However, by virtue of section 146 TULCRA, workers have a right not to be subjected to detriment by their employer for the sole or main purpose of preventing, deterring or penalising a worker from joining a union, taking part in union activities, or

¹⁰⁵ See the TUC's Report, "*Technology managing people: The worker experience*", op. cit. supra, page 33.

¹⁰⁶ It should also be noted that Article 11 of the ECHR (the right to association) will be engaged where a worker or employee's freedom to join and participate in a trade union is limited in some way; see [National Union of Belgian Police v Belgium](#) (App No. 4464/70, 27 October 1975). Trade union membership is also considered a special category of personal data under Article 9 of the GDPR. Processing of such data is prohibited unless one of the exceptions in Article 9(2) of the GDPR is established.

¹⁰⁷ Section 143(1) of TULRCA limits the scope of protections relating to recruitment to employees, whereas Section 152 of TULRCA on dismissal explicitly refers to employees.

making use of union services.¹⁰⁸ An employer would therefore be liable if it decided to terminate a worker's contract or not to contract with a worker on the basis of AI data regarding union membership or activities. The protection under section 146 also applies to employees.

2.115. Employees and workers in these circumstances would be able to take complaints to the Employment Tribunal. However, to bring a successful claim, they will generally have to prove that their union membership or activities were either the *reason* or *purpose* for the treatment complained of.¹⁰⁹ Difficulties will therefore arise where transparency around AI data used in the relevant decision-making process is lacking. This leads to our final conclusion in this Chapter.

Conclusion 15: There is adequate legal protection in relation to the protection of trade union activities. However, these rights will be enforceable only in so far as there are meaningful obligations in relation to transparency concerning AI, ADM, and related technologies.

¹⁰⁸ In *Ministry of Defence v Jeremiah* [1980] ICR 13, the Court of Appeal considered detriment to mean "putting under a disadvantage". Detriment has been held to include failure to promote an individual, refusal for training or other opportunities, reductions, or failure to increase pay, and disciplinary measures.

¹⁰⁹ There are provisions and principles which can assist claimants in this regard. Regarding refusal of employment, *Neckles v London United Busways Ltd* EAT 1339/99, the EAT held that if an employer was unable to provide a satisfactory explanation where the primary facts indicated an employee was refused employment on trade union grounds, an inference could be drawn that this was the reason for the refusal. In the context of dismissal, the burden is on employees with less than two years' continuous service to show that the dismissal was for a prohibited reason (*Smith v Hayle Town Council* [1978] ICR 996). However, where an employee has two years' continuous service, the burden is on the employer to prove the reason for dismissal was potentially fair (and not therefore based on trade union grounds). Further, the Supreme Court in *Royal Mail Group Ltd v Jhuti* [2019] UKSC 55 held that it is the duty of a tribunal to penetrate through an invented reason to uncover the real reason an employer dismissed an employee.

Chapter 3 – Recommendations for action and reform

Summary

In [Chapter 2](#) we analysed the existing legal system to understand how effectively existing laws regulated the use of AI and ADM in the workplace, primarily through an examination of case studies drawn from the *Worker Experience Report* and academic research.

In this Chapter, we set out why we consider that there is now an important opportunity for the TUC to play a formative role in shaping the legal protections and tools available in the workplace for regulating AI, ADM and ML so as to ameliorate the various deficiencies we have identified and ensure that the “*red lines*” we mapped out in [Chapter 1](#) are respected.

We make 17 specific recommendations aimed at legislators, regulators, and the trade union movement, explaining the principles that we believe should shape the future of regulation.

The present opportunity to shape the legal landscape

- 3.1. Although 2020 and 2021 will forever be seen as the years of the pandemic, the developing importance of these new technologies is not going completely unnoticed at the level of policy development within government. Thus, as well as the important work of the CDEI, in January 2021, the [Office of Artificial Intelligence](#) published a “*UK AI Council: AI Roadmap*”¹¹⁰ (“**the Roadmap**”), which recognised the need to examine new and different regulatory strategies to create public trust in helpful forms of AI. This Report noted that:

¹¹⁰ A copy of the Office of Artificial Intelligence publication “UK AI Council: AI Roadmap” is available [here](#).

It is clear that there remains a fundamental mismatch between the logic of the market and the logic of the law. Technology markets extract value from collective data while laws respond to individual opportunities and threats. This has a critical impact on the public acceptability of data as infrastructure – data supported by people, processes and technology – and will only worsen if it is not sufficiently addressed. One method that could begin to combine new forms of innovation and accountability is to involve the public in considering new ways to complement individual rights-based approaches such as consent. These would include new ways of ensuring public scrutiny of automated decision-making and the types of transparency that lead to accountability: revealing the purposes and training data behind algorithms, as well as looking at their impacts. They would include public engagement, including in algorithmic impact assessments. And they would look to ensure that existing regulations and regulatory bodies had not only the capacity but also the capability to fully consider the implications of AI in areas such as labour, environmental and criminal law. These three tenets: (1) clear transparency about automated decision making, (2) the right to give meaningful public input and (3) the ability to enforce sanctions could be encapsulated in a Public Interest Data Bill.

- 3.2. Whilst neither the Office of Artificial Intelligence nor any governmental body has yet proposed any *specific* legislation, the support for regulation is to be welcomed. The Roadmap highlights that the UK is currently at a crossroads and must choose which regulatory path to walk down. This means that currently there is a golden opportunity for the TUC to play a leading role in shaping the legal protections and tools available in the workplace for regulating AI and ADM.
- 3.3. The reference to the Public Interest Data Bill in the Roadmap as a possible regulatory strategy is particularly interesting. The Roadmap includes a link to an academic paper, published by authors based in the US, that explains more about how such a Bill would operate.¹¹¹ It provides this helpful summary of the proposal:

¹¹¹ Tisné, M., 2020. [The Data Delusion: Protecting Individual Data Isn't Enough When the Harm Is Collective](#). *Luminate*, July 2020.

A Public Interest Data Bill

1. Clear transparency:

1. Require that firms and governments open up the data and source code behind high-risk algorithms and define which are deemed “high-risk” in relation to evidence on the disparate impacts of those algorithms on the population (e.g. whether they fall disproportionality on marginalised communities).

2. Require that firms and governments publish algorithmic impact assessments assessing the outcomes of the algorithmic treatment on groups as well as any collective data-driven harms. Ensure the results of such assessments are published openly. Ensure these precede the rollout of high-risk AI deployments and renew these on a regular schedule.

3. Ensure full transparency and accountability of automation:

1. Tweaks to algorithms that might seem small or insignificant when considered alone, can add up to substantial collective impact when taken together – they would be included. These should not be limited to ‘decisions’ made by an algorithm nor to those decisions needing to be ‘significant’ as is currently the case with GDPR article 22.

2. Apply both to decisions that are fully, as well as partly automated.

3. Require transparency and accountability for how a decision was made based on a computer model, not simply explaining the model in abstract. (The degree and the mode of contribution of the algorithmic processing to the decision taken.)

4. Cover decisions beyond those that use personal data. For example, this would cover self-driving cars, or data that was once personal and then supposedly anonymised. People are impacted by data that is not personal, and by personal data that is not about them.

2. Public participation:

1. Provide members of the public with the possibility to give meaningful input into the use of automated decision making (including but not limited to input into algorithmic impact assessments).
2. Ensure that public participation is empowered and not merely consultative.
3. Sanctions:
 1. Ensure the ability to enforce sanctions for non-compliance.
 2. Fund and resource accountability bodies adequately, including oversight bodies for sectoral laws such as labour law, criminal law, genetic law, environmental law and discrimination, in addition to data protection agencies.
4. Relevance to groups as well as individuals:
 1. Enable persons as well as organisations to lodge requests.
 2. Provide access to the treatment parameters and, where appropriate, their weighting, applied to the situation of the person(s) or groups concerned.

- 3.4. The emphasis given in this proposed Public Interest Data Bill on viewing the regulation of AI and data through a collective lens and creating transparency and accountability is wholly consistent with our conclusions in [Chapter 2](#) and complements the recommendations we outline in this Chapter. It also reflects many views expressed internationally that the time for regulation of AI systems and associated technologies cannot be put off much longer.

Promoting the case for better regulating AI and ADM in the workplace

- 3.5. Before setting out our list of recommendations, we shall explain how we suggest that the TUC identifies the right way in which AI and ADM in the workplace should be further regulated. It is important to note here that there are some things that cannot be tolerated if human dignity at work is not to be

undermined. The implications of a failure to regulate will be profound for us all: as we said in the Introduction, that would lead to world “*where everything about us happens without us*”.

- 3.6. We have noted in [Chapter 1](#) the “*red lines*” that we suggest the TUC should adopt, and we strongly urge the TUC to take these as foundational points about which it will not negotiate. We discuss the implications of these in this Chapter. Once these are agreed, the next step is to consider what changes or actions flow from them. There is no one single approach that we can say is “right”, since it is the destination not the path that ultimately matters, but we can set out our thoughts and proposals on approaching the way forward.
- 3.7. Of course, the TUC is not itself a legislative body, so its approach must be to find a means to engage with like-minded organisations to press for the changes that it wants to see in the light of the *Worker Experience Report*. It must, of course, adapt its approach to the political weather as this will surely change over time, so we recognise that anything that we say in this Report as to the best strategy for the TUC will have to be somewhat general. Nonetheless, we think that there are some points we can usefully make about developing a strategy for reform.
- 3.8. Our analysis in the previous Chapters has *not* demonstrated that there is a total lack of available useful legal provisions to protect employees and workers. There are indeed gaps and there are also problems concerning the efficacy of some of the measures that exist. The *first* task therefore for the TUC is to take all possible steps to ensure that employees and workers can *now* make full use of the available protections, while also identifying how those gaps can be filled most swiftly and efficiently in the future. This is where strategy and tactics require separate consideration.
- 3.9. Given the increasing current awareness of the problems associated with AI, an argument can certainly be made for a wholly new enactment specifically addressed to AI, ML and ADM in general. A good argument can be made for this on a tactical basis, because it could have the effect of driving the discussion of the effects of AI systems higher up the public agenda. However, we do not think that this should be the overall strategy of the TUC for several reasons.
- 3.10. First, this approach – arguing for a major new legal instrument – demands legislative time in Parliament, but the time for significant major Bills – already

at a premium before the pandemic – is likely to remain limited as Parliament catches up with the business it has not been able to conduct properly while MPs have had to work remotely. So we do not think it is likely to be an effective or efficient route to make the significant changes we consider necessary and urgent.

- 3.11. Second, and no less importantly, our analysis in [Chapter 2](#) shows that much of the existing Labour Code and UK Data Protection legislation can be used right *now* to give some not insignificant protection to job applicants, employees and in some cases workers.
- 3.12. Third, the history of the development of this Labour Code has been one of accretion by legislation identifying and addressing new problems as they present. There is a long-standing practice of reform and change in this way.
- 3.13. The development of AI and ML are already seen as having such a role to play in the future economic development of this country that we think the strategy most likely to be successful may well be to build on the current framework and seek to reform those aspects which are not currently “fit for purpose” in light of the radical changes created by the Fourth Industrial Revolution.
- 3.14. There is a possible present opportunity for this approach. One proposal, outlined in the Queen’s Speech from December 2019,¹¹² is for the introduction of a new Employment Bill. More discussion of this is currently on foot, so this could provide an opportunity for the TUC to campaign for specific reforms to existing legislation based on our Report and the *Worker Experience Report*.
- 3.15. Of course, in the end, what matters is what works to secure reform; the decisions about this are certainly ones for the TUC’s executive and not us. Yet, whatever approach the TUC takes, we also recommend that the TUC and unions champion initiatives by way of collective bargaining and seek agreement from non-departmental public bodies such as ACAS for those soft-law tools that could be deployed to help ensure that AI and ADM are used lawfully, accurately, rationally, ethically, and appropriately in the workplace.

¹¹² A copy of the Queen’s Speech, 19 December 2019, is available [here](#).

Guiding principles that should shape regulatory reform

- 3.16. We turn now to consider the guiding principles that, in our view, should shape legal reforms and practical tools that are necessary.

“Red line” limits should not be negotiable

- 3.17. The “red lines” we identified in Chapter 1 must be embedded within the legal system. These “red lines” ensure that the fundamental tenets of the modern employment relationship are maintained, such as the principles of mutuality, trust and confidence, and transparency. These principles are not for negotiation.

“High risk” applications must be regulated

- 3.18. Next, we emphasise that the initial focus on new regulatory initiatives should be aimed at where there is a “high risk” of harm to the interests of workers and employers.¹¹³
- 3.19. One of the challenges when it comes to regulating AI and ADM effectively is ensuring that it is targeted at the right forms of technology. Many forms of AI or ADM will be entirely innocuous. Accordingly, there needs to be some basis on which AI and ADM is identified for legal regulation and we consider that identifying those applications that are “high risk” to workers and employees is the right place to start. When we use this phrase “high risk”, we mean those uses of AI and ADM that involve the processing of data, usually personal data, that produces or could produce legal effects concerning the worker or employee, or

¹¹³ For examples of regulatory proposals that target high-risk applications of AI, as opposed to universally application regulation, see (i) the German Data Ethics Commission’s seminal Report [“Opinion of the Data Ethics Committee”](#) available in English and summary form, (ii) The European Parliament’s Committee on Legal Affairs document [“Draft Report with recommendations to the Commission on a Civil liability regime for artificial intelligence”](#) (2020/2014(INL) and (iii) the European Commission consultation Report [“White Paper: On Artificial Intelligence – A European approach to excellence and trust”](#) COM (2020) 65 final.

similarly significant effects.¹¹⁴ When assessing if systems are “*high risk*” the focus is on the impact that the technology has on the individual worker, employee or job seeker.¹¹⁵ That is, those applications of AI and ADM that are inconsistent with the personal relationship built on mutual trust and confidence at the heart of the modern employment relation as explained in [Chapter 1](#). Our view is that the examples we have analysed in the Case Studies in [Chapter 2](#) would certainly fall within the definition of “*high risk*”.

- 3.20. Were this approach to be adopted, we recommend that sector-specific Codes of Practice should be developed that explain clearly and in detail which uses of AI, ADM and profiling would be “*high risk*” and how to identify them.

Regulation must be targeted

- 3.21. Regulation also needs to be targeted in the right place. We have seen how employers purchase proprietary systems with little knowledge of the way they work and the impact they can have on the employment relationship.
- 3.22. We know that employers will sometimes seek to displace responsibility for adverse effects on to the provider; so the control of AI systems needs to take into account the complexity of these systems and the fact that while some employers will use bespoke systems developed in-house, which should include better oversight of the development process, many will not. It is therefore critical that regulation encourages employers to take a great interest in the effects of the systems that they purchase and places obligations on organisations that develop systems even if they are not the ultimate “*end user*”.

¹¹⁴ The definition of “*high risk*” used in this Report echoes [Article 22 of the UK GDPR](#) although it is different in that it is not dependent on the extent of human involvement and we are keen to ensure that AI and ADM which impacts on individuals, even though personal data is not processed is encapsulated in this definition.

¹¹⁵ While writing this Report we were made aware of strong concerns, especially from the education sector, concerning the extent to which teaching professionals are being required to work in new ways that impact on student personal data. Whilst it is outside of the remit of this Report, we recognise that individual employees and workers may have their own employment rights infringed, for example in relation to the mutual term of trust and confidence, in so far as they are required or expected to process the personal data of third parties in a way that is unethical. More about the challenges faced by increased datafication in higher education is set out in “[The Automatic University: A review of the datafication and automation in higher education](#)”, UCU, June 2020.

Enhanced rights to data reciprocity must be established

- 3.23. Although, to a very significant degree, ownership of data at work lies with employees, it is employers who profit from it by, for instance, streamlining processes, facilitating decision-making, or training AI systems. This occurs because of the unequal bargaining power between employer and employee that Lady Hale noted in the passage we quoted in [Chapter 1](#).
- 3.24. The increasing degree to which employers seek to collect, manipulate, and then use workplace data is already having an adverse effect – from the employees’ point of view – on this already unequal relationship. We do not accept that this has to happen, and we are clear that the TUC should adopt a policy that seeks to address this change, to halt it and, if possible, to reverse it.
- 3.25. Accordingly, regulation should be premised on the understanding that data flows should be reciprocal and not simply a “one way street”. Reciprocity in this context means ensuring that employees and workers can access all the data that emanates from them, collate it to protect their own interests, and use it to their benefit. This change should be aligned with a proper mechanism by which employees can monitor and understand and how their data is being used.
- 3.26. In practical terms this will require an effective mechanism by which employees can access and combine this data, and that is likely to mean through the agency of their trade union representatives and the resources that the unions can bring to this task.

Regulation must be proportionate, practical, certain, and workable for all

- 3.27. It would be real mistake to conclude that all data use is to the disadvantage of employees and workers.
- 3.28. It is obvious that all involved with the employment relationship (employers, employees, workers, job applicants, trade unions, recruiters, advertisers, developers, regulators etc) need have legal certainty and practical guidance in relation to what amounts to the lawful, ethical, and sustainable use of AI and ADM.

- 3.29. Much data use can be highly beneficial in helping employees to increase their productivity, to eliminate tedious tasks, and to simplify otherwise difficult or onerous tasks. So, we are equally clear that legal regulation needs to work for employers too. Unless legal regulation is workable, practical, certain, and proportionate, it will be resisted and hamper “good” uses of AI and ADM. We do not subscribe to the view that introducing regulation of the use of AI systems in the workplace is a zero-sum game in which any gain for one side of industry is matched by an equivalent loss to the other.
- 3.30. The TUC will need to seek to build a consensus about how this is to work, and this should recognise some of the issues we have mentioned from the employers’ point of view. Perhaps the most important of these is that the “*black box*” problem can be a problem for employers too. Where an employer purchases a bespoke system, it would be wrong to think that it should *always* know exactly how that system works. For some this would be a practical impossibility and they will need to rely on the assurance of the seller, which in turn would have to rely on the competence of the developers and so on. So, we consider that legal regulation should encourage all actors in the “*value chain*” to develop and use AI and ADM in a lawful and ethical manner.
- 3.31. It should be recognised that employers, and organisations that develop products and tools for them, should be able to utilise useful and ethical AI and ADM across Europe without needing to overcome inconsistent or widely differing regulatory approaches. This consideration aligns well with our recommendation that legal regulation is first targeted at “*high risk*” applications of AI and ADM since such an approach is consistent with the initiatives that are currently being explored in Europe.
- 3.32. It needs to be borne in mind at each stage that there is also a strong interest in AI-specific regulation by legislators outside of the UK. The European Commission has embraced regulation in the hope that it will protect European values but also encourage investment. The Council of Europe has also focused on regulation as a means of ensuring that the benefits of technological progress are not at the expense of fundamental values. Globally, some countries have introduced AI laws too. Regulation that is consistent across jurisdictions is likely to be accepted far more readily by employers. This means that, despite Brexit, it would be wrong for the UK to simply ignore what is happening in Europe.

A pre-emptive approach to governance should be established

- 3.33. New initiatives should encourage a pre-emptive approach to governance in which a multi-stakeholder approach is created, with the unions playing a substantive role in partnering with employers.¹¹⁶ We consider that placing a multi-stakeholder approach at the heart of the deployment of “*high risk*” forms of AI and ADM will better ensure that these new forms of technology are used in an ethical, lawful, and non-discriminatory way.

New initiatives should be established collectively

- 3.34. New initiatives should harness the collective power of the trade union movement. Much of the harm created by AI and ADM arises from the power imbalance between employer and workforce; collective power can go some way to remedying these difficulties.

General recommendations for legislation

- 3.35. It is the guiding principles and the various “*gaps*” in legal protection identified in [Chapter 2](#) that underpin our recommendations for legislation and for further action.

1: The amendment of UK data protection legislation to enact a universal right to explainability in relation to “*high risk*” AI or ADM systems in the workplace with a right to ask for a personalised explanation along with a readily accessible means of understanding when these systems will be used.

¹¹⁶ For a general example of a multi-stakeholder governance model, see the World Economic Forum’s ideas within [“How to put AI ethics into practice: a 12-step guide”](#).

Meaningful information

- 3.36. In order for trade unions, employees and workers to understand whether data is being processed ethically, lawfully and without discrimination, there should be an obligation to provide meaningful information about the logic involved, as well as the envisaged consequences of such processing for the data subject in relation to all decisions taken about workers, employees or potential workers or employees involving “*high risk*” applications of AI or ADM.¹¹⁷ “*High risk*” AI tools or ADM systems that cannot provide this level of explanation simply should not be utilised in the workplace.

Section 1 particulars

- 3.37. To ensure that a worker has ready access to information about how AI and ADM are being used in the workplace in a way that is “*high risk*”, we recommend that employers are obliged to provide this information within the statement of particulars required by section 1 of the Employment Rights Act 1996 as supplemented by sections 2 to 7 of that Act.¹¹⁸

AI registers

- 3.38. Further, employers should be obliged to maintain a register that contains this information, and which would need to be updated regularly, perhaps annually.¹¹⁹ This register would be readily accessible to existing employees, workers, and job applicants, including employees and workers that are posted to sites controlled by organisations other than the employer.

¹¹⁷ This idea has been championed by other organisations, for example The German Data Ethics Commission “[Opinion of the Data Ethics Committee](#)”, see recommendations 46 to 76, and also the ETUC’s document entitled “[Artificial Intelligence: Will it make bias against women worse?](#)”.

¹¹⁸ Section 1 onwards of the Employment Rights Act 1996 can be accessed [here](#).

¹¹⁹ An obligation for information provision has been explored by the European Commission in its first consultation “[On Artificial Intelligence – A European approach to excellence and trust](#)” at page 20. This idea is also recommended by the German Data Ethics Commission, “[Opinion of the Data Ethics Committee](#)”, see recommendation 45.

- 3.39. Whilst we appreciate that employers routinely create Privacy Notices that provide information about data processing, we understand from the TUC's AI Working Group that these are often difficult to locate and many employees and workers will not even understand that these documents exist and contain important information pertinent to the employment relationship. This problem is particularly acute where workers and employees perform their work "offsite" on third parties' premises such that their data is processed away from their own employer. Our recommendations would ensure that transparency around data processing was clearly embedded and situated within the employment relationship, in essence translating the requirements within the UK GDPR into the reality of the working world.

2: The Employment Rights Act 1996 should be amended to create a right, which can be enforced in the Employment Tribunal, for workers not to be subject to detrimental treatment, including dismissal, due to the processing of inaccurate data.

A right not to suffer detriment from inaccurate data or other breach of data regulation

- 3.40. We recommend that a new cause of action is created within the ERA 1996 to prevent employees and workers from being subjected to a detriment in consequence of the processing of inaccurate data, or other data breach.¹²⁰ This new right would be analogous to the existing detriments claims contained in sections 47A to 47G although it would also extend to dismissals. It would ensure that workers and employees were protected from the adverse

¹²⁰ An obligation for technically robust and accurate AI systems has been explored by the European Commission in its first consultation paper "[On Artificial Intelligence – A European approach to excellence and trust](#)" at pages 20 to 21. The German Data Ethics Commission also promotes this idea in the context of statistical models in its "[Opinion of the Data Ethics Committee](#)", see recommendation 51. This theme is further explored by The Chartered Institute for IT in its September 2020 Report, "[The Exam Question: How do we make algorithms do the right thing?](#)" examining the fallout from the use of algorithms to determine A Level results. It argues that the developers of systems need to be clear that statistical models are used in a way which create a *just* outcome especially where standardisation processes are deployed.

consequences of inaccurate data being processed by an employer – or its agent – regardless of the individual’s status or length of service.

3: The UK’s data protection regime should be amended to state that discriminatory data processing is always unlawful.

- 3.41. AI-powered technologies are difficult to regulate because their use cuts across many different areas of law. The focus of this paper has been the interaction of employment law, equality law and data protection principles as contained in the UK GDPR and DPA. Of course, AI-powered technologies affect other areas of law such as public law, child protection and consumer rights, but that is not this Report’s focus. The law, to meet the challenge of regulating AI, must “*fit together*” cohesively to ensure a holistic and consistent approach. One glaring disconnect within the existing patchwork of legal regulation is the failure within UK data protection legislation to link the principle of non-discrimination with data protection principles. The UK GPRR and DPA do not contain an express statement that discriminatory data processing as understood by the Equality Act 2010, whether fully automated or otherwise, is unlawful.¹²¹
- 3.42. To resolve this disconnect between the DPA/UK GDPR and the Equality Act 2010, we recommend that the DPA expressly states data processing is not lawful where it is discriminatory as defined by the Equality Act 2010 and that there can be no exceptions to that principle.¹²²

¹²¹ This omission is unfortunate as the UK GDPR does address the potential for data processing to be discriminatory and makes it plain that it will be unlawful in the context of fully automated tools in [Recital 71 to the UK GDPR](#).

¹²² This is an idea that was also explored in the Report by The Law Society, “*Algorithms in the Criminal Justice System*” from June 2019 within section 6.

4: The burden of proof in relation to discrimination claims which challenge “high risk” AI or ADM systems in the workplace should be expressly reversed.

- 3.43. We recommend that there is a complete and express reversal of the burden of proof in relation to “*high risk*” uses of AI or ADM systems, such that the employer must prove from the outset that discrimination has not occurred rather than the conventional burden of proof in discrimination claims where the claimant bears the initial burden albeit in the context of a shifting burden of proof: section 136 Equality Act 2010.¹²³

5: Provision should be made to ensure that all actors in the “value chain” leading to the implementation of AI and ADM in the workplace are liable for discrimination subject to a reasonable step defence

- 3.44. Determining the point at which discrimination has been introduced into an AI tool, or becomes an issue, can be problematic as we have noted in [Chapter 2](#) and which formed Conclusion 2. Various solutions have been offered to this difficulty such as the imposition of strict liability on the organisation that ultimately utilises the AI system to the creation of legal mechanism which targets the “*manufacturer*”.¹²⁴
- 3.45. In our view, for discrimination claims brought under the Equality Act 2010, we consider that a different solution is appropriate. While not ruling out the possibility of strict liability, we consider that the approach should be that all parties in the “*value chain*” should have the potential to be sued in the Employment Tribunal, but also that each such actor can defend any claim on

¹²³ The European Trade Union Confederation (ETUC) has called for the complete reversal of the burden of proof in its statement, “[Humans must be in command](#)”.

¹²⁴ A useful summary of the competing positions is contained in chapter 3 of the House of Commons Science and Technology Committee’s “[Algorithms in decision-making](#)”, Fourth Report of Session 2017-19, on 23 May 2018.

the basis that they took all reasonable steps to prevent the discrimination occurring.¹²⁵

- 3.46. This type of defence already exists in the Equality Act 2010 but only in relation to employers who are vicariously liable for the discriminatory actions of their employees: see [section 109 \(4\) Equality Act 2010](#). This provision (which has been in place in some form since 1975) has proved effective in changing cultures in the workplace towards the maintenance of an equality culture. We see no reason why it should not be extended in this way and we think that it could also advance the kind of culture of responsibility about the use of AI systems that we have advocated already. In short, we believe that extending this defence to all actors involved in the development of AI and ADM tools that are then used in the workplace will encourage everyone to take proactive steps to minimise the risk of discrimination at every step in the development process.

6: No international trade agreement should protect intellectual property rights from transparency in such a way as to undermine the protection of employees and workers' rights.

- 3.47. This recommendation relates to the concerns already expressed that Digital Trade Agreements will undermine the basic regulation of AI systems outlined in [Chapter 2](#) within Conclusion 4. There are several ways in which this Recommendation can be taken forward by the TUC. At the very least the TUC needs to ensure that, perhaps with the ETUC and the ITUC, it is involved in the discussions around such agreements so that it can scrutinise them as to their potential to cause harms. The TUC can try to ensure that there are political commitments within the UK that match those which are being developed within the European Union. Taking the issue further, it would be possible to develop a statutory provision that limited the prerogative of governments to make treaties.

¹²⁵ The idea of imposing liability throughout the “value chain” is explored in the European Commission’s consultation paper, [“Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics”](#).

7: Equality Impact Audits in the workplace should be made mandatory as part of the Data Protection Impact Assessment process and made readily accessible to workers, employees, and their representatives.

- 3.48. Data Controllers like employers are under an obligation by virtue of Article 35 of the UK GDPR to conduct a Data Protection Impact Assessment (DPIA) where data processing is likely to result in a *“high risk to the rights and freedoms of natural persons”*. Whilst DPIAs were created with the intention that they would examine *“an assessment of the risks to the rights and freedoms of data subjects”* and Recital 75 to EU GDPR does list *“discrimination”* as a relevant risk,¹²⁶ we understand from the TUC’s AI Working Group that DPIAs do *not* routinely examine the extent to which discrimination is occurring. We recommend that statutory guidance is produced as a matter of urgency to clarify that DPIAs must include Equality Impact Assessments.¹²⁷ Moreover, there should be an obligation on employers to publish all DPIAs in a way that means they can be readily and easily accessed by workers, employees, and their

¹²⁶ An excellent guide has been produced by Prospect on how DPIAs should be conducted entitled [“Data Protection Impact Assessments: Guide for union representatives”](#) which highlights the importance of making an assessment in relation to the risk of discrimination.

¹²⁷ The notion that an auditing process should be extended to all AI systems and include discrimination is not a new idea along with the notion that these risk assessments should be made public; these ideas have been advocated for by many organisations, for example see (i) the UK Government’s [“Guidelines for AI procurement”](#), which indicate that an AI impact assessment should be initiated at the project design stage and all critical decision points so as to examine the *“human and socio-economic impacts of your AI systems”* along with *“data quality”* and the potential for *“inaccuracy or bias”*, (ii) the German Data Ethics Commission’s seminal Report [“Opinion of the Data Ethics Committee”](#), which is available in English, strongly advocates auditing in respect of *“self-determination, privacy, bodily integrity, personal integrity, assets, ownership and discrimination”*, (iii) it is a requirement of Canada’s [“Directive on Automated Decision-Making”](#), (iv) it is promoted by AI Now in its seminal document [“Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability”](#), (v) the CPSL also endorses the use of AI impact assessments that should be mandatory in the public sector and publicly available is its February 2020 Report entitled [“Artificial Intelligence and Public Standards”](#) (Recommendation 7), (vi) the House of Commons Science and Technology Committee’s Report [“Algorithms in decision-making”](#), Fourth Report of Session 2017-19, on 23 May 2018, paragraph 52, also recommends auditing, (vii) the IFOW has produced a document, *“Artificial Intelligence in hiring: Assessing impacts on equality”*, (viii) The Chartered Institute for IT strongly argued in its September 2020 Report [“The Exam Question: How do we make algorithms do the right thing?”](#) that publicly available auditing was key and (ix) risk assessing AI systems for matters like discrimination was advocated by UNI Europe in its 2019 paper [“UNI Europe ICTS: Position on Artificial Intelligence”](#).

representatives. The best way of achieving this objective should be addressed in statutory guidance.

8: Provision should be made for joint statutory guidance on the steps that should be taken to avoid discrimination in consequence of these new technologies.

- 3.49. We strongly recommend that statutory guidance is developed on a cross-disciplinary basis between the EHRC, CDEI, ACAS, ICO, CBI and TUC to plainly explain to organisations the ways in which discrimination can arise in the employment relationship as a result of new forms of technology such as AI and ADM.¹²⁸
- 3.50. This type of practical guidance is needed to ensure that employers, trade unions, employees and workers are fully aware of the risk that AI and ADM pose to the principle of non-discrimination and that steps can be taken to identify those risks and avoid them. This legal reform would hopefully minimise the risk of discriminatory data processing and decision-making.

9: There should be statutory guidance for employers on the interplay between AI and ADM in relation to Article 8 and key data protection concepts in the UK GDPR.

- 3.51. Despite the potentially far-reaching legal consequences of AI and ADM, there is a lack of case law and legally binding guidance to employers as to the scope

¹²⁸ The CDEI Bias Review (op. cit. supra) contains numerous recommendations aimed at regulators and government to the effect that guidance should be issued which explains the risk of algorithm discrimination and biases. It is a matter for discussion whether this is adequate, but it is certainly a step forward given the lack of any such guidance at present.

of key data protection concepts that AI-powered technology can impact on, a matter we identified in [Chapter 2](#) within Conclusions 5 to 9.¹²⁹

3.52. We recommend that practical statutory guidance is produced that addresses, as a minimum, the following concepts:

- The protection which workers and employees enjoy under Article 8 in relation to monitoring, profiling and surveillance by AI-powered tools and ADM, especially when they are working from home and/or are being used to make judgments about the type of person an employee is assessed to be, for example, hard-working, lazy, fraudulent.
- The circumstances in which an employer can lawfully process data on the basis that it is “*necessary*” to the employment contract under Article 6(1)(b) of the UK GDPR.
- The circumstances in which an employer can lawfully process data on the basis that it is “*necessary*” to protect their legitimate interests or those of a third party under Article 6(1)(f).
- The interplay between Article 6(1)(b) and (f) bearing in mind that the lawful basis for data processing dictates the extent to which Articles 21 and 22 can be invoked, and these provisions include important safeguards in relation to the use of AI-powered technologies and ADM.
- The circumstances in which Articles 21 and 22 can be disapplied.

3.53. This recommendation is entirely consistent with section 128 of the DPA, which empowers the Secretary of State to require the Information Commissioner to produce Codes of Practice in relation to the processing of personal data.

3.54. We recommend that statutory guidance through a Code of Practice is produced as a matter of urgency to protect the interests of workers and create certainty for employers. There should also be real significance attached to failures to

¹²⁹ Indeed, it is worth noting that the ICO’s Employment Practices Code has not even been updated in light of the DPA 2018. A copy is available [here](#) and the supplementary code is [here](#). It also does not address AI or ADM.

follow said Code of Practice, with the potential for civil or even criminal liability. Trade unions should be consulted on the creation of the Code of Practice, as envisaged by section 128 which states that the Information Commissioner must consult organisations that represent the interests of data subjects.

10: There should be a statutory right for employees and workers to disconnect from work so as to create “*communication free*” time in their lives.

- 3.55. To protect workers and employees from the constant expectation to be available for communication with their managers or colleagues, which can have a negative impact on mental health, we propose a right to disconnect so as to create a protected personal space for employees and workers where they cannot be contacted or expected to communicate unless it is necessary. We recognise that the practicalities of such a right would look different dependent on job role, seniority, and sector. Accordingly, we propose that there should be an obligation on employers to engage with their workforce as to how best to map out, define and protect a “*communication free*” space for workers.

11: There should be a comprehensive and universal right to human review of decisions made in the workplace that are “*high risk*”.

- 3.56. We identified in [Chapter 2](#) within Conclusion 12 that the personal nature of the employment relationship is threatened if there is no automatic entitlement to a human review of decisions that are made about workers and employees. Accordingly, we recommend here that [section 14 DPA](#) is amended so that all decisions made in the workplace that are “*high risk*” carry with them an

entitlement to ask for a human review.¹³⁰ That is the absolute minimum but in our view it ought also to include an opportunity to actually engage in person with an individual representing the management of the company. We address this in the next Recommendation.

12: There should be an express statutory right to personal analogue engagement – an “in person engagement” – in relation to decisions made in the workplace which are “high risk” such as may have any significant impact on the working life of employees and workers.

- 3.57. Machines and technology are not human, and we cannot have a personal relationship with them in the same way that we can and do with other humans. It is fanciful to suggest otherwise even though this may be a goal of those developing AI systems. They can only be an aid to human interaction if the employment relationship is to remain personal and built on mutual trust and confidence. Employees are entitled to more than just a “relationship” with a machine.
- 3.58. We recommend that the TUC press for legislators to clarify that all employees have a right to that personal relationship whenever these new technologies are deployed in the workplace in relation to workplace decisions that are “*high risk*”. In practice, this means that employees and workers should have a right to insist that they can interact with a human being rather than a machine or algorithm in relation to “*high risk*” decisions. For example, job applicants seeking a new role or existing employees facing redundancy decisions could insist that they are interviewed and marked by a human rather than simply talking aimlessly into a screen. We do not accept that employees and workers should ever be treated as mere units of production nor that they can be

¹³⁰ The notion that humans should play a leading role in AI systems is mainstream. It is explored by the European Commission in its first consultation paper in relation to certain AI applications “[On Artificial Intelligence – A European approach to excellence and trust](#)” at page 21. See also the [ETUC statement “Humans must be in in command”](#) and the German Data Ethics Commission “[Opinion of the Data Ethics Committee](#)”, recommendation 71 “...As a general rule, therefore, systems should be designed in such a way that a human can override technical enforcement in a specific case”.

compelled in effect to contract with systems or machines. This kind of relationship has been rightly called an “in person engagement”.

Recommendations concerning a bipartisan approach to data rights

13: Employees and workers should have a positive right to “data reciprocity”, to collect and combine workplace data so as to better understand the ways in which new technologies are being and can be used in the workplace, and to take advantage of this information for themselves.

- 3.59. Lady Hale discussed “*the significant imbalance of power between the contracting parties as there often will be in an employment contract*” as outlined in [Chapter 1](#). This is evident in the asymmetry between the power of the employer to collect and use data in relation to its workers and the inability of employees to reciprocate.
- 3.60. There is an assumption that, subject to the current existing controls, it is the employee or worker that gives away the data and the employer that uses it. We think that this assumption needs to be challenged. Why should it be only that way around? There ought to be wholly reciprocal obligations both in theory and in practice.
- 3.61. In a workplace there is much data that an employee or worker would benefit from having and knowing. To a very limited extent this has been considered in the context of Gender Pay Reporting obligations.¹³¹ In many cases an AI system will have been used to create the information that is needed to fulfil these obligations.
- 3.62. However, it has been argued that such outtakes from the pay records of a firm do not give a useful picture for the workers and are more cosmetic for the firm.

¹³¹ See the [Equality Act 2010 \(Gender Pay Gap Information\) Regulations 2017](#), which apply to all private and voluntary sector employers with 250 or more employees, and the Equality Act 2010 (Specific Duties and Public Authorities) Regulations 2017 apply to specified English authorities, specified cross-border authorities and specified non-devolved authorities across England, Scotland and Wales.

Employees are given only generalised information about the pay levels and the numbers of persons in the organisation. The information is not enough to be very useful. At most it may help a worker to challenge an employer as to whether there is truly an equal pay system, but it will probably never be enough to demonstrate unequal pay.

- 3.63. There is therefore a strong argument that employees and workers should collectively be entitled to collect data on issues, such as pay, in exactly the same way as employers. In short, there should be a requirement that an employer can obtain consent to use data only if a reciprocal right is given to the worker. In this way the employee or worker is empowered to be on equivalent footing with the employer. Such a right would be useful not only in the context of equal pay, but also in situations where redundancies are threatened and choices have to be made based on performance standards.
- 3.64. No doubt some employers might voice objections to this, but one lesson is clear about the use of these new technologies by employers to date; they are developed mainly to advantage the employer rather than the employee. By giving workers practical rights to data reciprocity, to collect and use this kind of information, there would be some restoration in the power relationship between the two sides of industry.
- 3.65. This legal reform, which would create a positive right for workers and employees to access their data and combine it on a collective level across the workforce, will go some way to ensure a fair balance between employer and employee. It might also allow discriminatory, unethical, or inaccurate AI and ADM to be exposed.

14: Trade unions should have a formal data-gathering role in relation to member data so that they can effectively monitor the use of “high risk” AI and ADM in the workplace.

- 3.66. A further response to the power imbalance created by data is for trade unions to adopt a formal data-gathering role.

- 3.67. There is no reason why data collation should be the preserve of employers provided that the UK GDPR and DPA are followed. Gathering data in this way could enable the identification of problems, which analysed individually might not be apparent.¹³² The trade union movement must be best placed to facilitate this form of data aggregation and analysis from a worker and employee perspective. It may also be able to use its resources to ensure that workers have access to the expertise and insight of data scientists who specialise in how to gather and interpret data.
- 3.68. It is possible that trade unions, wanting to harness the power of data, will need to embark on internal training programmes to upskill their officials and may also need to engage with data scientists to understand how best to analyse data gathered. However, this is the reality of a new world in which data is increasingly at the heart of many activities and enterprises.

15: Trade unions should seek recognition as data subject representatives under the UK GDPR.

- 3.69. A related point is that in order to ensure that information gathered by unions can be acted on, we further recommend that trade unions seek and are granted legal rights that entitle them to bring claims, on behalf of data subjects, where “high risk” uses of AI or ADM has led to infringements of data protection principles.

¹³² An interesting example of the power of collating data in order to identify and tackle discrimination, a problem which is often best understood from a collective rather than individual stand point, was highlighted in the *Financial Times* on 23 July 2020 in a piece entitled [“Race and America: why data matters”](#). The journalist recounts the story of Yeshimabeit Milner, who began collecting data on suspensions in a neighbouring school and found that black children were four times more likely to be suspended than white children. She now leads an organisation called Data for Black Lives. The idea of using data to advance social good has also been explored by the Turing Institute, for example [“Opportunities to use untapped data science to support social, economic and financial inclusion”](#) and [“Workers of the Internet unite? Online freelancer organisation among remote gig economy workers in six Asian and African countries”](#).

3.70. At present, certain associations may claim this status under Article 80 of the UK GDPR with a mandate from the data subject. The Article states that:

1. The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.
2. Member States may provide that any body, organisation or association referred to in paragraph 1 of this Article, independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority which is competent pursuant to Article 77 and to exercise the rights referred to in Articles 78 and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing.

3.71. Article 80 (1) is replicated with minimal additional detail within [section 189 DPA](#).

3.72. We consider that the trade union movement would be well placed to litigate breaches of the UK GDPR on behalf of its membership, especially with the benefit of a "*bird's eye*" view of data that would be created by the adoption of Recommendation 14.¹³³

¹³³ Please note that the Government launched a consultation exercise in relation to section 189 Data Protection Act 2018 towards the end of 2020 as outlined [here](#).

Recommendations concerning collective bargaining and a multi-stakeholder approach

16: There should be a statutory duty to consult trade unions in relation to the deployment of “*high risk*” AI and ADM systems in the workplace directly or through a third party.

- 3.73. To strengthen the oversight of “*high risk*” AI and ADM systems, there should be a statutory duty on employers to consult with trade unions in relation to decisions to implement and use “*high risk*” AI and ADM systems, whether directly or through a third party.

17: Employment-focused ethical principles in relation to “*high risk*” AI and ADM systems should be established.

- 3.74. A parallel, sometimes alternative, narrative that has developed within the AI policy landscape is the reliance on ethical standards to regulate new forms of technology as opposed to legal rules.¹³⁴
- 3.75. At present, there is no universally accepted set of ethical principles for the regulation of AI and ADM. Indeed, there is a vast array of different and competing ethical codes in circulation which are permitted by different organisations. These have been helpfully collated and referenced by Algorithm Watch as part of its AI Ethics Guidelines Global Inventory.¹³⁵

¹³⁴ The ETUC has also gone one step further, calling for a set of legally binding ethical principles, see the ETUC statement, “[Humans must be in in command](#)”.

¹³⁵ Algorithm Watch’s AI Ethics Guidelines Global Inventory can be accessed [here](#).

- 3.76. This diversity of views as to the right ethical approach to adopt has led the Committee on Standards in Public Life to recommend in its February 2020 Report entitled “*Artificial Intelligence and Public Standards*” that the Government should clarify which ethical standards should be followed in the public sector and how they work in practice.¹³⁶ This follows a similar recommendation from that of the House of Commons Science and Technology Committee in May 2018, in which it highlighted that “*there is currently no unified [ethical] framework for the private sector*”.¹³⁷
- 3.77. We believe that the trade union movement is very well placed to put forward a definitive view of how ethical principles should be articulated in the context of the employment relationship and we recommend that it urgently undertakes that work.
- 3.78. A comprehensive and practical set of ethical guidelines for the use of “*high risk*” AI and ADM in the workplace could lead to the normalisation of ethical behaviour and a common understanding of the acceptable uses and deployment of new forms of technology.
- 3.79. Moreover, a comprehensive set of ethical guidelines would sit in parallel to, and enhance, the existing (and hopefully improved) legal framework, creating flexible, practical, and dynamic guidance to employers, trade unions, employees, and workers. Again, the trade union movement could use its unique access and perspective on the challenges faced by workers and employees to construct ethical guidelines that would be particularly meaningful and considered. It could also work with colleagues in the ETUC to ensure that the ethical principles were universal within Europe.

¹³⁶ A copy of the Report is available [here](#).

¹³⁷ The House of Commons Science and Technology Committee, “[Algorithms in decision-making](#)”, Fourth Report of Session 2017-19, on 23 May 2018, paragraph 51.

About the authors

[Robin Allen QC](#) and [Dee Masters](#) are both practising barristers specialising in employment law, equality, and human rights law. They work internationally and have conducted litigation at every level, and on every protected ground under UK and EU law. They have also lectured and trained jurists across Europe on issues relating to equality.

They set up the [AI Law Consultancy](#) because they were increasingly aware of the potential dangers in the rapid proliferation of AI systems and associated new technologies. Initially they believed that AI would primarily impact upon the provision of goods, facilities, and services. However, it became very clear, especially after the Covid-19 pandemic, that AI and ADM would have a significant impact on the workplace in terms of data protection principles, privacy, and equality. This meant that businesses, trade unions and individuals needed clear, well thought through advice to navigate the rapidly changing technological and legal arena. Their website contains information about the developing regulation of AI systems and is updated frequently. They also tweet about these developments at [@AILawHub](#).

Working together as the AI Law Consultancy, they have significantly contributed to the discussions on the regulation of AI systems; as well as drafting this Report their work in 2020 included:

- The influential 2020 Report for Equinet, “[*Regulating for an Equal AI: A New Role for Equality Bodies: Meeting the new challenges to equality and non-discrimination from increased digitalisation and the use of Artificial Intelligence*](#)”.
- Working with the Council of Europe in 2020–21 to write and deliver a training programme in relation to AI and discrimination for regulators both in the UK and across Europe.
- Working with the UK’s Centre for Data Ethics and Innovation in the preparation of its “[*Review into bias in algorithmic decision-making*](#)”, 2020.



Published by
Trades Union Congress
Congress House
Great Russell Street
London WC1B 3LS

tuc.org.uk

March 2021

ISBN: 978 1 911288 91 6

© 2021 Robin Allen and Dee Masters all
rights reserved, but reproduction is permitted
provided both the copyright holder and the
TUC is acknowledged.

The views expressed in this publication belong to the
authors. The information contained therein is not intended
as legal advice and should not be relied upon as such.
The authors and the TUC are not liable for use that may
be made of the information contained therein.

Design by TUC
Cover photo by Getty Images