
ELA Annual Conference 2021

The legal implications of Artificial Intelligence & related technologies in the workplace

Robin Allen QC & Dee Masters

www.cloisters.com / www.ai-lawhub.com

HAND OUT

Over the summer of 2020, the TUC launched the first-ever survey of the ways in which UK employers were deploying Artificial Intelligence, Automated Decision Making and other forms of technology in the workplace: [Technology managing people: The Worker Experience](#) (“**the Worker Experience Report**”). It found that these forms of technology were being used at every stage in the employment relationship and, in many cases, there was little understanding of its legal implications by managers and staff. As we shall discuss this was a mistake; the legal issues arising from the use of these technologies in the work context are really extensive.

To complement the Worker Experience Report we were asked by the TUC to report on the legal implications of the uses that it recorded. It has been published on 25 March 2021 here: [Technology Managing People – the legal implications](#) (“**the Legal Implications Report**”). We hope that ELA members will read that report for its the detailed analysis.

This handout does not repeat the detailed legal analysis in the Legal Implications Report. Rather it has been written to complement the live session for the ELA Annual Conference on 17 May 2021 - [AI in the Workplace](#). The handout aims to provide an easy and accessible guide which contains: [key terminology](#), [litigation to date](#), [legal checklists](#) ([discrimination](#), [implied term of trust and confidence](#), [unfair dismissal](#), [privacy](#)), an identification of “[hot spots](#)” where particular care is required due to a higher risk of legal non-compliance, and some points on [future developments](#) in this fast evolving area. It should also be borne in mind that these new forms of technology are fundamentally about data so that the UK GDPR and Data Protection Act 2018 is also likely to apply more generally.

KEY TERMINOLOGY

1	<i>Artificial Intelligence</i> – Conceptual definition
<p>There are many definitions of AI. We think a good place to start is the conceptual definition coined by Professor Frederik Zuiderveen Borgesius - "<i>the science of making machines smart</i>".¹ This phrase perfectly encapsulates why AI matters to employment lawyers. 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. This is precisely why AI is becoming more and prevalent at all stages of the employment relationship from the time consuming process of recruitment to employee monitoring to dismissal.</p>	
2	<i>Artificial Intelligence</i> - UK definition
<p>AI and related concerns are yet to be defined in the UK in the context of the employment relationship.</p> <p>But there is already one current UK statutory definition of AI - although that concerns regulation by the Competition and Markets Authority of certain business transactions - in section 23A(4) of the Enterprise Act 2002.</p> <p>It defines AI to mean "<i>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.</i>"</p>	

¹ Zuiderveen Borgesius, F., 2018. [Discrimination, artificial intelligence, and algorithmic decision-making.](#)

3	<i>Artificial Intelligence</i> – Proposed EU definition
<p>There is a proposal within Europe to regulate AI. The European Commission has proposed defining “artificial intelligence system” (AI system) as meaning “... <i>software that is developed with one or more of the techniques and approaches listed in Annex 1 and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with</i>”.</p> <p>Annex 1 contains a detailed list of approaches and techniques for the development of AI to be adapted by the Commission in line with new technological developments.</p> <p>Key participants across the AI value chain are also clearly defined such as providers and users of AI systems that cover both public and private operators to ensure a level playing field.</p>	
4	<i>Algorithms</i>
<p>At the heart of AI is the algorithm. They are the logical steps, created by programmers, that instruct a computer to use a data input and to create an output often by comparing the input with other data which the computer has already processed.</p>	
5	<i>Machine learning</i>
<p>Machine learning is certainly one of the most significant features of AI systems; it is what creates “<i>intelligence</i>”.</p>	

The International Association of Privacy Professionals (**IAPP**) has neatly described machine learning in the “[The privacy pro's guide to explainability in machine learning](#)” –

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.

Facial Recognition Technology is a form of machine learning algorithm in which a system has learnt to recognise a human face by “*learning*” what a person looks like through an analysis of vast sets of databases of faces.

6 Automated Decision Making

When AI or an algorithm is used to make decisions or where conclusions are reached that have an effect, without any direct, or with only limited, human involvement, it is called Automated Decision Making or ADM.

ADM will often sit alongside Artificial Intelligence, for example, when a passport gate matches your face to your passport (Facial Recognition Technology); a computer and not a human allows you to pass through the gate.

7 Profiling

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, which define it under Article 4(4) of the UK GDPR 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.

Profiling is increasingly happening in the workplace to answer questions like: Is an employee a trustworthy employee? Is this person likely to be a good employee?

8 Biometric identification

Another problematic area is the collection and analysis of biometric information by artificial intelligence or machine learning systems.

In the UK, biometric data is defined within the Protection of Freedoms Act 2012 to mean any information about a person's physical or behavioural characteristics or features. This can be used for a variety of reasons in the workplace such as controlling access and egress, location and work monitoring. This almost always engages Article 8 ECHR and is often subject to specific statutory controls under data protection provisions in relation to biometric data.

Examples in the workplace: facial recognition technology², voice recognition technology³ etc.

SIGNIFICANT LITIGATION TO DATE

Here is an overview of the litigation in the UK and Europe to date concerning either the use of AI / algorithms in an employment/work context or where there have been equality dimensions.

1	<p>R (on the application of Edward Bridges) v The Chief Constable of South West Wales Police [2020] EWCA Civ 1058</p> <p>A judicial review brought by Liberty which challenged the use of Facial Recognition Technology by the police. Some equality arguments were considered especially the Public Sector Equality Duty but fundamentally a case about data rights and the human rights and public implications of Facial Recognition Technology.</p>
2	<p>Foxglove, a new law firm interested in making technology fair, challenged the Home Office's algorithm for fast tracking visa applications on behalf of the Joint Council for the Welfare of Immigrants (JCWI) on the basis that it was racist. The Home Office agreed to stop using the algorithm before any court hearing.</p>

² A useful summary of the technology and its use can be found in the [CDEI Snapshot Paper – Facial Recognition Technology](#).

³ The CDEI published a [Snapshot Paper on Smart Speakers and Voice Assistants](#).

3	<p>R (on the application of The Motherhood Plan and anor) v Her Majesty's Treasury [2021] EWHC 309 concerned a judicial review brought by The Motherhood Plan (otherwise known as “Pregnant then screwed”) which challenged the HM Treasury’s Self Employment Income Support Scheme (SEISS) scheme on the basis that it is discriminatory. Our blog considering this decision is here.</p>
4	<p>In Filcams Cgil Bologna and others v. Deliveroo ITALIA S.R.L.⁴ the Bologna Court had to consider an app that Italian Deliveroo used to decide the priority it afforded the company’s riders in relation to access to jobs.</p> <p>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.</p> <p>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. Our blog considering the decision is here.</p>

⁴ See Case N. R.G. 2949/2019 *Filcams Cgil Bologna and others v. Deliveroo ITALIA S.R.L.*, judgment of Dr. Chiara Zompì, 31 December 2020, available in Italian [here](#).

5	<p>System Riscico Indicatie, or SyRI for short, is a controversial risk profiling system that was deployed in the Netherlands by the Department of Social Affairs and Employment with the intention of identifying individuals who are at a high risk of committing fraud in relation to social security, employment and taxes. The algorithm at the heart of SyRI was developed to analyse a wealth of governmental data which included: work/ trade / employment information, name, address, age, gender, postcode (which can be a proxy for race), and health data.</p> <p>A broad coalition of civil society organisations and individuals started litigation against the Government over the use of SyRI. It was argued that SyRI breached the right to private life, the right to privacy, the GDPR and the right to an effective remedy due to the lack of transparency around the algorithm itself. As part of the arguments concerning transparency, it was argued that the system could not be interrogated so as to ensure that discrimination was not occurring which, on its fact, must be contrary to public law principles.</p> <p>It concluded that Article 8 had been breached and whilst the Court did not go on to find that discrimination was <i>actually</i> occurring, it did conclude that the <i>possibility</i> of discrimination combined with an absence of transparency fortified its conclusion that Article 8 had been breached. Our detailed blog is here.</p>
6	<p>A group of uber drivers sought access to data - using the GDPR - concerning the way in which algorithms “managed them”.</p> <p>Importantly, Spain is about to introduce new legislation which will force companies to open the “black box” and reveal algorithms to gig workers.</p>
7	<p>In the Employment Tribunal, we are only aware of one group of cases, in which we represent the Claimants, where equality/fairness arguments are being advanced on behalf of employees. These cases, which involve the dismissal of women by a machine with no human decision-making and an absence of transparency, will be heard in late 2021 or early 2022.</p>

The relative lack of litigation should not lull employment lawyers into a false sense of security. There are many parallels between the extensive equal pay litigation of recent decades and the operation of AI in the workplace (lack of transparency, lack of knowledge, the potential for group claims, the potential for significant compensation within group litigation). We are very

much aware of issues being investigated across the UK and Europe about the deployment of these systems in the workplace.

LEGAL CHECKLISTS

Please note that the regulation of AI is a quickly moving areas and these Checklists are likely to expand and shift. They should be a beginning and not the end of an analysis. They can be used by both sides of industry. Note if there is a cross Border issue where there is deployment in the UK and EU 27 it would be sensible to discuss with the AI Law Consultancy how developing EU law might be relevant.

Discrimination

The full range of discrimination under the EA 2010 is possible in the employment relationship from recruitment through to dismissal. For example, in the US, academic research 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.⁵ Other research has also demonstrated that women are less likely to be shown adverts for high-paying roles in general.⁶ Academics have also highlighted how AI powered recruitment tools may fall foul of the duty to make reasonable adjustments by failing to accommodate people who speak or present differently.⁷

AI systems are often hidden within “black boxes” meaning that employers may not even understand that discrimination is occurring or what data is being processed. 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.⁸ This means that, paradoxically, the lack of meaningful transparency as to the way

⁵ 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 also Gerards, Janneke and Xenidis, Raphaële [Algorithmic Discrimination in Europe. Challenges and opportunities for gender equality and non-discrimination law](#) European Union 2021.

⁶ 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.

⁷ [Disability, Bias, and AI](#), 2019, AI Now Institute.

⁸ 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.

in which an algorithm or AI or machine learning model works, might *assist* claimants who are prepared to litigate without having certain evidence of discrimination.

Direct discrimination – s.13 Equality Act 2010		
Q1	<p>Does the artificial intelligence system treat people differently because of a protected characteristic?</p> <p>This could be for various reasons, such as direct bias in the code used, or in the data set to which it is applied, or because machine learning has treated a particular personal characteristic as a proxy for gender, race ethnicity etc.</p>	Direct discrimination
Indirect discrimination – s.19 Equality Act 2010		
Q2a	Does the artificial intelligence system consist of an algorithm and / or is it trained on a data set that places certain protected groups at a disadvantage (a PCP)?	If so, there is <i>prima facie</i> indirect discrimination.
Q2b	If so, can the employer using the artificial intelligence system point to a legitimate aim to justify the use of the algorithm and / or data set?	Assess the extent to which there is a defence to <i>prima facie</i> indirect discrimination
Q2c	If so, is the artificial intelligence system capable of achieving the aim?	Assess the extent to which there is a defence to <i>prima facie</i> indirect discrimination
Q2d	<p>If so, is the artificial intelligence system a proportionate means of achieving the aim?</p> <p>Consider always:</p>	Assess the extent to which there is a defence to <i>prima facie</i> indirect discrimination

	<p>Is there a non- or less discriminatory means by which the aim could be achieved?</p> <p>Does the system comply with relevant ethical standards such as transparency and explainability?</p>	
Transparency		
Q3	<p>What information is available to assess the answers to Q1 to Q2 above?</p> <p>Has any audit been carried out?</p> <p>Are there national or pan-European laws such as the GDPR / UK GDPR which will allow employees or workers to understand more about what is going on?</p> <p>Is the system so lacking in transparency / explainability that the courts are entitled to infer <i>prima facie</i> discrimination?</p>	Consider the evidential burden
Other types of equality claim		
Q4	<p>Are there other equality type claims that could be brought, such as, harassment or a failure to make reasonable adjustments or a breach of s.15 Equality Act 2010?</p>	Assess further legal breaches
Liability issues		
Q5	<p>Who is the party responsible in law?</p>	Identify the right respondent

	This would certainly be by the employer but might other commercial third parties be liable – e.g. by acting as agents of the employer by implementing the AI system.	
Q6	Does the employer benefit from any indemnity with any third party supplier of data sets or the algorithms etc?	Assess extent of liability

Implied term of trust and confidence

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.

Every employment contract is subject to an implied term of mutual trust and confidence: [Malik and Mahmud v. Bank of Credit and Commerce International S.A.](#)⁹ 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: [Keen v Commerzbank AG](#).¹⁰ 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.

This obligation of mutual trust and confidence has other important consequences for any analysis of the implications of Artificial Intelligence systems on the workplace. 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*, paragraphs 44 & 110).

⁹ 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](#).

¹⁰ [2006] EWCA Civ 1536, [2007] IRLR 132, [2006] 2 CLC 844, [2007] ICR 623, see [here](#).

An employer is also required to take decisions about employees in way that is **lawful, rational** and in **good faith**: *Braganza v BP Shipping Limited*.¹¹ Indeed, the actions of employers can be subject to closer **scrutiny** than the parties to a simple commercial contract (*Braganza*, paragraph 55).

Q1	<p>In using an artificial intelligence system, is the employer acting lawfully?</p> <p>Consider in particular obligations under the Equality Act 2010 and UK GDPR concerning data processing.</p>
Q2	<p>Does the artificial intelligence system make and support rational decision making?</p>
Q3	<p>Does the artificial intelligence system make and support good faith decision making?</p>
Q4	<p>Does the artificial intelligence system permit the employer to explain adequately the decisions it makes about its staff?</p>
Q5	<p>Is the decision discriminatory?</p>
Q6	<p>Does the decision breach fundamental rights (data protection rights) or Article 8?</p>

¹¹ [2015] UKSC 17, [2015] IRLR 487, [2015] ICR 449, [2015] 1 WLR 1661, see [here](#).

Unfair dismissal

Employers obviously have a statutory obligation under the Employment Rights Act 1996 to **act fairly** in terms of **process** and **outcome** when dismissing employees with over two years' continuous service remains.¹² It is not watered down in any way just because business has utilised new ways for human resource management.

Q1	Does the employee have unfair dismissal rights?
Q2	Does the employee know that an artificial intelligence system is being used?
Q3	What criteria does the artificial intelligence system use? (Hint: if the employer doesn't even know, it probably isn't fair)
Q4	What data does the artificial intelligence system use? (Hint: if the employer doesn't even know, it probably isn't fair)
Q5	Can the employer be sure that the artificial system is not selecting employees by reference to protected characteristics either directly or indirectly? See discrimination checklist.
Q6	Is the employee disabled and require reasonable adjustments? If so, can and how does the artificial system make that adjustment? How can the employer be sure that any adjustment is appropriate?
Q7	Can the artificial intelligence system explain why the employee has been dismissed in sufficient detail that the decision can be understood by a layperson and effectively challenged?

¹² See Part X of the Employment Rights Act 1996, see [here](#).

Q8	Did the dismissal arise from any employee monitoring which might infringe Article 8?
Q9	Does the decision fall within the band of reasonableness test?
Q10	<p>Is the dismissal UK GDPR / Data Protection Act 2018 compliant?</p> <p>Check, in particular:</p> <ul style="list-style-type: none">• Lawful ground for data processing• Transparency rights• Article 22 (prohibition on some fully automated decision making)• Article 21 (limitations on semi-automated decision making)

Right to privacy

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. 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.¹³

The compatibility of the monitoring with Article 8 therefore turns on whether the inference can be justified under Article 8(2).

¹³ See the TUC’s Report, “[Technology managing people: The worker experience](#)”, page 27.

Q1	<p>Is Article 8 engaged?</p> <p>Intrusive processing of employee personal data, especially whilst employees are compelled to work at home, for the purposes such as productivity monitoring will fall within the scope of Article 8.¹⁴ It is also possible that surveillance which accesses personal data will constitute an interference with employees' privacy rights under Article 8.¹⁵</p>
Q2	<p>In using the artificial intelligence system lawful?</p> <p>Consider in particular obligations under the Equality Act 2010 and UK GDPR / Data Protection Act 1998 concerning data processing.</p>
Q3	<p>Does the artificial intelligence system pursue a legitimate aim?</p> <p>Note: It is well-established that employers have '<i>a legitimate interest in ensuring the smooth running of the company, and that this can be done by establishing mechanisms for checking that its employees are performing their professional duties adequately</i>'.¹⁶</p>
Q4	<p>Is the interference with Article 8 necessary in a democratic society?</p>
Q5	<p>Is it proportionate?</p> <p>This stage of the justification defence requires a detailed examination of the facts before any final decision as to whether Article 8 has been breached can be made. It follows that whether a violation can be established will be highly fact sensitive</p>

¹⁴ 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](#)).

¹⁵ See [Antovic and Mirkovic v Montenegro](#) (App No. 70838/13, 28 November 2017); [Amann v Switzerland](#) (App No. 27798/95, 16 February 2000).

¹⁶ See [Barbulescu](#).

	The factors below will be relevant in determining whether the monitoring of employees is proportionate to this interest.
Q6a	Has the employer notified the employees of the nature and scope of the monitoring?
Q6b	What is the extent of the intrusion into the employees' privacy?
Q6c	Has the employer provided legitimate reasons for the monitoring?
Q6d	Could a less intrusive form of monitoring been used?
Q6e	How effective is the monitoring in ensuring the smooth running of the employer's business?
Q6f	What are the consequences of the monitoring on the employees?
Q6g	Are there adequate safeguards in place?
Q6h	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?

“HOT SPOTS”

The checklists outlined above should always be considered when assessing the impact of Artificial Intelligence and related technologies. The table below outlines the “hot spots” where there is likely a higher risk of legal non-compliance and so where great care in advising is necessary. The AI Law Consultancy can always help on specific problems here.

Any actions which are not readily observable or transparent

AI and ML systems can often be applied to employees or potential recruits in ways that are not readily observed, such as the process of CV scraping or deciding which adverts job seekers are presented. While artificial intelligence and machine learning might be observable in theory (maybe, for example, it's flagged in a privacy notice), the way it works will often be far from transparent. Great care is needed in these situations to apply the Checklist especially as a lack of transparency might shift the burden of proof in discrimination cases.

Recruitment / dismissal decisions

AI is increasingly used to recruit and dismiss employees such that there is minimal human interaction between the job applicant and the employer. Machine algorithms can lead to discrimination and may not comply with minimal requirements in relation to fairness: see Checklists above.

Algorithmic management tools with insufficient discretion

One advantage of Automated Decision Making is that decisions which might be time consuming or repetitive can happen very quickly.

But these systems often come at a price which is an inability to make discretionary decisions. Like the Italian Deliveroo case identified above, there is the risk that if these systems do not have “a human in the loop” there will be discrimination or arbitrary and irrational decision making which is insufficiently personalised.

Decisions about disabled people

Similarly tools which make decisions about disabled people may not be sufficiently complex and nuanced to be able to identify and then implement the duty to make reasonable adjustments. Machine learning in particular may mean that systems are only geared to non-disabled people.

Biometric identification tools

Any use of biometric tools is particularly sensitive particularly when it is used to make predictions about people. Artificial intelligence and machine learning are being increasingly explored as a means of drawing conclusions about people using biometrics, for example, whether they are telling the truth, whether they are happy, or whether they are suitable for a job.

For example, [Faception](#) claims to use artificial intelligence and machine learning to analyse people’s faces in order to match them to the following personality types: “High IQ”, “Academic Researcher”, “Professional Poker Player”, “Bingo Player”, “Brand Promoter”, “White-Collar Offender”, “Terrorist” or “Paedophile”.

However - as explained in this influential [article](#) - machine learning does not distinguish between correlations that are causally meaningful and ones that are incidental. For example, the algorithm may have drawn a link between a particular item of clothing in an image and a certain character trait. It might be true that in most images which have been labelled as showing “a non-criminal” that the person is wearing a white shirt but this does not mean that wearing such a shirt indicates that a person is not a criminal.

FUTURE DEVELOPMENTS

<p>UK legislation?</p>	<p>To date, there is no AI specific legislation in the UK which focuses on the employment relationship. The closest we get to direct legal regulation of AI in the employment sphere is the UK GDPR / Data Protection Act 2018.</p> <p>In January 2021, the Office of Artificial Intelligence published a UK AI Council: AI Roadmap, which recognised the need to examine new and different regulatory strategies to create public trust in helpful forms of AI.</p> <p>The TUC has also published a manifesto and will be campaigning for more legal regulation in this area in the upcoming Employment Bill.</p>
<p>UK regulators?</p>	<p>There is a growing pressure on UK regulators to produce specific guidance following the CDEI's seminal review into algorithmic biases.</p>
<p>European Commission</p>	<p>A Draft Regulation was published in April 2021 which proposes fair ranging reform in the AI sphere.</p>
<p>Council of Europe</p>	<p>The Council of Europe has established a specialist committee – CAHAI – to examine the impact of AI and assess whether additional regulation is required. Draft proposals are expected.</p>

To stay up to date on future developments, please follow us at [@AILawHub](#) or sign up for our blogs [here](#).

ABOUT THE AUTHORS

Robin Allen QC and Dee Masters are specialist discrimination barristers based in London at [Cloisters chambers](#) with deep knowledge of the equality implications of artificial intelligence (AI) and algorithmic discrimination having written and lectured extensively on this area.

In 2019, they created www.ai-lawhub.com which is a centralised resource for tracking and analysing the emerging debate in the UK, Europe and globally concerning AI and the ways in which it should be analysed with an equality, data protection and human rights framework. They also tweet regularly from [@AILawHub](#) on developments in this area. Their blogs, which examine equality issues and AI are available [here](#).

Their work has been referenced by the European Commission and led to invitations to participate in discussions with various governmental and non-governmental bodies in the UK: the Equality and Human Rights Commission, the Committee on Standards in Public Life as part of their review of AI and its impact on public standards, the All Party Parliamentary Group on the Rule of Law (which examined the regulation of automated decision making) and the Centre for Data Ethics and Innovation (CDEI). Robin sat on the steering committee for the CDEI's recent seminal paper - [Review into bias in algorithmic decision-making](#) and Dee is currently sitting on a steering committee for the CIPD which will produce guidance aimed at employers deploying AI.

On the 10 June 2020, Equinet published their major Report - [Regulating for an equal AI : A New Role for Equality Bodies: Meeting the new challenges to equality and non-discrimination from increased digitisation and the use of Artificial Intelligence](#) - discussing the next steps in European regulation of AI systems.

During late 2020 and early 2021, Robin and Dee wrote and delivered a training programme for the Council of Europe, in conjunction with the CDEI, for UK regulators on discrimination and AI. It will soon be delivered to French regulators.

On 25 March 2021, the TUC published a legal opinion by Robin Allen QC and Dee Masters called [Technology Managing People – the legal implications](#).

They provide legal advice to employers and employee through their legal consultancy – the AI Law Consultancy.