CALL FOR EVIDENCE: GOVERNANCE OF ARTIFICIAL INTELLIGENCE (AI)

Response from the Employment Lawyers Association

24 November 2022

SECTION 1

REPLY TO HOUSE OF COMMONS SELECT COMMITTEE'S

CALL FOR EVIDENCE ON THE GOVERNANCE OF ARTIFICIAL INTELLIGENCE

24 November 2022

General

1. The Employment Lawyers Association ("ELA") is an unaffiliated and non-political group of specialists in the field of employment law. We are made up of about 6,000 lawyers who practice in the field of employment law. We include those who represent Claimants and Respondents/Defendants in the Courts and Employment Tribunals and who advise both employees and employers.

2. ELA's role is not to comment on the political merits or otherwise of proposed legislation. Policy decisions are for Government and the policy debate is for politicians and not for the expert employment lawyers who make up the membership of ELA.

3. In this paper, as expert employment lawyers, we have identified many issues in respect of the use of AI and its impact on employers, employees and in the workplace. We have then made many proposals to resolve the issues that we have identified. ELA should be clear that in making those suggestions and proposals below we recognise that their implementation and evaluation will require a political process requiring consultation with employers, employees, businesses, regulators and other stake holders that may reveal issues that we may not have identified or considered. As expert employment lawyers, ELA can identify the issues and make suggestions for their potential and pragmatic solution. ELA recognises however, that the final decisions on any such proposals are one for a political process including a number of other factors such as resources and many other evaluative judgments which political debate ELA does not enter into.

OUR FOUR KEY POINTS

A big risk to the employment relationship means a big need for effective governance.

4. AI potentially offers huge benefits but in employment law terms it carries substantial risks, particularly for employees and particularly in terms of equality. It goes to the heart of the legal basis of the employment relationship: trust and confidence.

5. If employees can't understand employers' decisions that affect them because those decisions are taken by complex software, it risks damaging that trust and confidence. That in turn may break both the relationship and the contract.

6. Everything we suggest is therefore about mitigating that risk so that employers can benefit from AI and employees be comfortable with it. Of course, we recognise employers and unions and other stakeholders in the workplace may have views on all our ideas. Our aim is only to identify the legal problems and suggest solutions that have the potential to reconcile everyone's interests.

An opportunity to work with the existing law

7. There are already provisions on the statute book that could be amended and expanded to give better clarity to employees, as individuals and as a workforce and minimise the risk of discrimination.

8. For example, the law already requires employers to give workers a 'statement of particulars': perhaps amend it to refer employees to their employer's policies and information about the AI the employer uses that affects them. Similarly, in certain circumstances employers are required to provide information to the workforce on certain issues including health and safety: perhaps amend those to include encourage employers to pass on information or consult about how the employer's AI technology makes decisions about them.

Workplace enforcement mainly looks back: perhaps it should look more forward

9. The protections for workers in the Equality Act 2010 and the data protection legislation apply to AI, even if they weren't designed for it. However, to enforce their rights, individuals have to bring a claim. That can be difficult and expensive, particularly where they have very limited information.

10. We suggest not just looking at mechanisms to give workers more information at a much earlier stage, but also question whether regulators should have powers to require employers and suppliers of AI to explain what it does, so that employers can pass that information on to the workforce.

Does the workplace need another regulator, specifically for AI?

11. The Government's preference is to work with existing regulators. We are not sure if that this is the best option.

12. The main regulators in the workplace in this context are the EHRC and the ICO, although there are others (such as the FCA) who may also have a stake. They can sometimes have competing policy objectives and neither seems properly resourced (both financially and in skillset) to deal with AI, the EHRC in particular.

13. We therefore suggest that this question is looked at again. In any event, if we are to rely on the current bodies, their remit and resources will need to expand and they may need to find a way of working together to avoid both overlap and conflict in their responsibilities.

SECTION 2

REPLY TO HOUSE OF COMMONS SELECT COMMITTEE'S CALL FOR EVIDENCE ON THE GOVERNANCE OF ARTIFICIAL INTELLIGENCE

1. How effective is current governance of AI in the UK?

What are the Current Strengths and Weaknesses of Current Arrangements, Including for Research?

1.1 Executive Summary

- There is no agreed definition of AI. Nor is there is currently any specific governance or regulation of AI in the workplace. AI is likelyk in respect of some of its functions and in this context, to fall primarily under the equality and data-protection legislation, but there are no specific provisions of that legislation which purport to govern or regulate it.

- Whilst both relevant regulators - the EHRC and the ICO – are looking at the impact of AI, we question if they are taking a joined-up approach and we question if either, and the former in particular, is or will be adequately resourced (financially and in respect of skillset) for the task. Perhaps, in order to avoid duplication, concentrate expertise and avoid conflicting objectives, a new single regulator for AI is required.

- Both the law and the regulators are only engaged after an alleged breach. This means enforcement is largely in the hands of individuals and only after the event. Given the potential adverse impact of non-compliant AI on many employees, we question if this can be said to be effective.

1.2 What is AI?

This is beyond ELA's remit to address. We suggest it may also fall outside the Committee's or indeed the Government's, with material implications for how AI is then governed and regulated. The lack of a comprehensive definition mitigates against AI-specific regulation. Any statutory definition risks being 'gamed' by actors who wish to remove software from outside the regulatory regime.

The AI pioneer and scientist John McCarthy in 2004 suggested:

"*It is the science and engineering of making intelligent machines, especially intelligent computer programs. It is related to the similar task of using computers to understand human intelligence, but AI does not have to confine itself to methods that are biologically observable*."

IBM suggested a definition for machine learning as follows:

"Through the use of statistical methods, algorithms are trained to make classifications or predictions, uncovering key insights within data… gradually improving its accuracy."
The European Commission proposal for regulation on AI (the "AI Act") may also be useful to illustrate the multiple potential definitions of AI:

"*software which is developed with one or more of the techniques and approaches listed [within a prescribed list] 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."*

The TUC say:

"Unfortunately, there is no single, agreed definition of AI, algorithm or machine learning. In our AI worker survey Technology Managing People, we used the following definitions, designed to be straightforward and accessible:

- *Artificial intelligence means when computers carry out tasks that you'd usually expect to be completed by a human. For example, making decisions or recognising objects, speech and sounds.*

- *Machine learning means when computer programmes are trained on data so that the programme can learn to carry out certain tasks.*

- *An algorithm used in technology is often a set of rules that a computer applies to make a decisio*n"

The multiplicity of definitions need not impede discussion of AI but in ELA's view it suggests an obstacle to the governance and regulation of AI per se in a purpose-designed legislative framework.

1.3 The use of AI in the workplace

Artificial intelligence can be deployed by an employer to assist with decision-making and staff management across the life-cycle of its relationship with its workers, from recruitment to termination.

To give just a few examples, AI can be used to:

a) sift through job applications by being calibrated to "read" CVs and make decisions on whether to shortlist a candidate for interview, against the parameters the AI has been "taught" to look for;

b) conduct initial interviews with prospective workers, with applicants answering questions posed by a chatbot in a video call;

c) support HR professionals in handling repeat tasks, by answering frequently asked questions from employees;

d) tailor training to an employee's specific areas of development, by monitoring employee activity and output, alongside their job description and the performance of their peers;

e) provide instructions to workers in carrying out tasks and monitor their performance against algorithmically-generated targets; and

f) assist a business in making decisions about who is allocated work or assigned a shift, imposing sanctions such as temporarily suspending workers from carrying out that work (and therefore impacting their earning potential) and ultimately, determining whether the relationship should be terminated.

From a recent survey conducted by one of our members, nearly half of overall respondents (47%) – and 53% of respondents from large companies – are either currently using technology solutions and/or AI to support their recruiting and hiring efforts (28%) or planning to in the next year (19%).[1]

1.4 Current governance structure

The legal framework underpinning the governance of AI in the workplace currently straddles employment law and data protection law.

In particular, the risk of algorithmic bias facilitating unlawful discrimination against job candidates and workers engages protections under the Equality Act 2010 ("**EqA 2010**"). Although AI-assisted decision-making can also touch other areas of employment law (for example, unfair dismissal protection and working time requirements), the pitfalls of over-reliance on AI are most obviously seen through the prism of equality law. A lack of understanding about how AI systems work and the risk of biased input data exacerbating human prejudice (despite best intentions to eliminate such prejudice) lend themselves to distrust regarding the efficacy of algorithmic analysis.

The use of an individual's personal data, both to make decisions about them specifically and as part of the input data that may be used to "train" and refine AI systems, is subject to an employer's obligations under the UK General Data Protection Regulation ("**UK GDPR**") and the Data Protection Act 2018 ("**DPA 2018**").

Alongside an individual's right to enforce protections under the EqA 2010, UK GDPR and DPA 2018 (see further below), there are two existing regulatory bodies:

a) in the discrimination field, the Equality and Human Rights Commission ("**EHRC**") was established under the Equality Act 2006. Amongst other things, it has a statutory duty to encourage good practice in relation to equality and diversity, enforce the EqA 2010 and promote awareness and understanding of rights under it. The EHRC is also required to monitor the effectiveness of equality law, advise the Government about such effectiveness and to recommend changes to the law. [Of course, the issue of equality extends beyond employment relationships. It is also relevant to service providers, whose use of AI may create bias that impacts customers (for example, in relation to the assessment of credit ratings). This will likely be relevant to other sector-specific regulators too];

b) in the data protection field, the role of the Information Commissioner (and its predecessors) has been in place since 1984. Their current remit to enforce and monitor data protection laws is set out in the DPA 2018 and the UK GDPR. These obligations are carried out by the Information Commissioner's Office ("**ICO**").

[1] https://www.littler.com/files/2022_littler_european_employer_survey_report.pdf

Neither the EHRC nor the ICO were set up specifically with the governance of AI in mind. We address certain specific issues relating to AI and GDPR in our response to Question 2 below. This issue is recognised more widely by the Department of Culture Media and Sport in its report on Establishing a pro-innovation approach to regulating AI (July 2022) (the "**DCMS Report**"):

"*AI is partially regulated through a patchwork of regulatory requirements built for other purposes which now also capture uses of AI technologies.*"

Notwithstanding this, it is evident from the proposals in the DCMS Report that it intends to rely on existing regulators to create sector-specific regulatory regimes, underpinned by cross-sectoral principles. Therefore, the onus will be on the EHRC and ICO, between them, to ensure effective governance of AI in the workplace under any new regulatory system.

There is also a multitude of advisory bodies, Government departmental sub-groups and independent organisations with direct interest and expertise in shaping AI governance and policy. These include the Office for Artificial Intelligence, the Regulatory Horizons Council, the Central Digital and Data Office, the AI Council, the Centre for Data Ethics and Innovation, the Alan Turing Institute, the Ada Lovelace Institute, the Open Data Institute and the AI Standards Hub.

Generally, they operate in a purely advisory capacity to Government and sector-specific regulators. They will often collaborate on areas of shared interest, contribute to policy-making and Government consultation exercises, appear before Parliamentary committees, commission research reports and develop non-binding guidance and standards across sectors. However, unlike the ICO and EHRC, they have no enforcement powers.

1.5 What does effective governance of AI look like?

We have outlined above some of the potential benefits of carefully deployed, targeted AI to augment human decisions and HR processes. When properly explained and applied appropriately, it may well be that AI can have a transformative positive effect on how workplaces operate, for the mutual benefit of employers and those who work for them. As matters stand it seems clear that the primary benefit is for employers and unless there is understanding, acceptance and consent from employees the benefits of AI may be qualified. The pervasive nature of AI in the workplace – and its potentially significant impact on the ability of individuals to earn a living and progress in their chosen field – places it towards the higher end of the risk spectrum.

It does not, of course, pose an existential risk to humans in the same way as, for example, a malfunctioning driverless car or an algorithm which facilitates inaccurate medical diagnoses. However, it does involve a real risk to people's way of life, their job security, their privacy and their aspirations. An employee's job is likely to be their primary economic asset. It directly engages individual rights enshrined in the European Convention for the Protection of Human Rights and Fundamental Freedoms, including the right to respect for private and family life (Article 8) and the prohibition of discrimination (Article 14).

The problem was summarised neatly by the All-Party Parliamentary Group on the Future of Work's Report on The New Frontier: Artificial Intelligence at Work (November 2021) ("**APPG Report**"):

"*A core source of anxiety is a pronounced sense of unfairness and lack of agency around automated decisions that determine access or fundamental aspects of work. Workers do not understand how personal, and potentially sensitive, information is used to make decisions about the work that they do; and there is a marked absence of available routes to challenge or seek redress. Low levels of trust in the ability of AI technologies to make or support decisions about work and workers follow from this. We find that there are even lower levels of confidence in the ability to hold the designer, developers and users of algorithmic systems meaningfully accountable for their responsible governance.*"

Addressing this problem requires an effective regulatory regime which focuses on three core stakeholder groups: the developers of AI tools in the employment sphere, the employers who deploy such technology in the workplace and the individuals (chiefly, job candidates and workers) who are potentially impacted by its use.

The DCMS Report has proposed an initial set of "cross-sectoral principles", to be interpreted and implemented in practice by existing regulators (such as the EHRC and the ICO). These are, in summary, to:

a) ensure that AI is used safely;

b) ensure that AI is technically secure and functions as designed;

c) makes sure that AI is appropriately transparent and explainable;

d) embed considerations of fairness into AI;

e) define legal persons' responsibility for AI governance; and

f) clarify routes to redress or contestability.

1.6 How effective are the current arrangements?

The cross-sectoral principles outlined above provide a good benchmark for assessing the effectiveness of the current governance of AI in the workplace.

This exposes several weaknesses and gaps in the current system. In particular:

a) **No accepted definition of AI**: In order to put in place effective governance and regulatory arrangements, it is first necessary to be clear on how "artificial intelligence" should be defined. Without this, it is very difficult for a regulator (or those who are regulated) to understand the real scope of any governance structure and when it applies. At present, there is no commonly accepted definition.

b) **Reliance on individual enforcement**: Although the EHRC and ICO each has regulatory powers, the effective upholding of rights under the EqA 2010, UK

GDPR and the DPA 2018 often relies on individual enforcement through the employment tribunals and civil courts. By its nature, the current system is largely focused on providing remedies for breaches of employment, equality and data rights, after they have occurred. It relies on disgruntled individuals having the resources, know-how and determination to see the process through.

c) For many individuals, pursuing litigation is prohibitive in terms of the cost (and the risk of adverse costs in a losing case), time and stress involved. Further, without proper transparency and a system of quality assurance for AI systems, they may be largely unaware that algorithms are being applied to make decisions about them (possibly to their detriment) and/or that their personal data is being used to refine automated processes. Alternatively, data subjects may also pursue litigation because they suspect wrongdoing. Without effective enforcement there is little deterrent to persuade data controllers to voluntarily change systems which purportedly breach the rights of data subjects.

d) **Misalignment of regulatory powers**: Effective regulation in this area will require a coherent, joined-up approach from the ECHR and ICO. This will not be assisted by the current disparity in their respective enforcement mechanisms. For example, the ICO has the power (amongst other things) to issue fines directly to employers for data breaches. The ECHR cannot do this for discriminatory behaviour (although it does have certain other enforcement tools at its disposal). This means that the scope for a certain type of regulatory intervention depends on whether the impact of an AI system results in unlawful discrimination or an identifiable data breach – and, in each case, whether the ICO or EHRC considers it is a cause worth pursuing.

e) The DCMS Report recognises that it should consider "*if there is a need to update the powers and remits of some individual regulators. However, we do not consider that equal powers or uniformity of approach across all regulators to be necessary*". Given that governance of AI in the workplace operates at the intersection between employment and data protection law, there is a case for greater alignment in approach between the EHRC and the ICO on AI-related matters.

f) **Lack of consistency**: The EHRC and the ICO appear to be at different stages when it comes to engagement on AI issues – at least in terms of the published material. Both have much wider (and very different) remits but where they converge on AI, the ICO appears to have been much more active. This is perhaps understandable, given the specific provisions in data protection legislation in relation to automated decision-making (and is not a reflection on the valuable role of the EHRC). However, this lack of consistency is a potential weakness in current AI governance.

g) Although the EHRC has identified "*addressing the equality and human rights impact of digital services and artificial intelligence*" as one of its six core priorities in its *Strategic Plan: 2022-2025*, there has been limited published activity to date (see our answer to Question 3). It has produced some guidance on *Artificial intelligence in public services*, but this is relatively short and focused solely on the public sector. There are also no published investigations by the ECHR into the use of AI in the workplace.

h) In contrast, "*artificial intelligence, big data and machine learning*" was identified as one of the ICO's top three priorities at an earlier stage, in its *Technology Strategy 2018-2021*. In addition, the ICO has produced multiple pieces of guidance, including its *Guidance on AI and Data Protection* (July 2020), *Explaining decisions made with AI* (May 2020) and an *AI and Data Protection Risk Toolkit*. (considered in more detail in our answer to Question 3)

i) **Lack of AI-focused regulation**: The UK Government is still getting to grips with how it wishes to regulate the use of AI. Our current laws did not contemplate the wholesale introduction of AI into the workplace but they do largely reflect a social and political consensus as to appropriate protections for employees,

j) The APPG Report included persuasive arguments for "*a simple, new corporate and public sector duty to undertake, disclose and act on pre-emptive Algorithmic Impact Assessments*", enshrined in a new Accountability for Algorithms Act. There are also lessons to be learned from other jurisdictions, which have adopted a legislative approach to some degree.

k) The DCMS Report endorses a different approach. This will focus on cross-sectoral principles (such as those outlined above), with regulators asked to consider lighter touch options, such as guidance and voluntary measures, in the first instance. It is unclear whether this will be effective in addressing the discrimination and other employment-related risks associated with AI. Either way, we would suggest that the government may wish to address the current vacuum as a priority.

l) Barriers to employee engagement: Employers are unlikely to engage with their staff (or their representatives) effectively where they do not understand the scope and operation of AI systems in order to provide meaningful consultation. Some employee representative forums may not have sufficient technical knowledge of AI systems to be able to represent effectively the interests of their members or constituents. Further, the current laws on information and consultation may not give employees a sufficient platform to understand how new technologies are being deployed, have their say on whether they should be implemented and (crucially) contribute their views on the purpose and design of such systems and the data being used to "train" them. Employee and wider public trust is crucial to the success of AI in the workplace – and yet, in our experience, AI systems are currently being deployed without input from important stakeholders (namely, those who will be impacted by decisions made in relation to their personal circumstances). This being despite the requirements placed upon data controllers under UK GDPR, DPA 2018 and other employment law rights explained below.

m) Insufficient quality assurance / explainability: As the proposed cross-sectoral principles illustrate, effective governance is more than simply providing means of redress when things go awry. It requires regulators to take steps to prevent things going wrong in the first place. In particular, we recommend that the EHRC and ICO need to consider how to ensure that AI is technically secure and functions as designed, is appropriately transparent and explainable and is embedded with considerations of fairness to the rights of data subjects.

n) We suggest they will need to assess what level of intervention is appropriate to provide quality assurance (and public reassurance) that AI is operating as intended. This means striking a balance between:

   i. an arms-length approach of detailed voluntary guidance to developers and employers, where this is proportionate in lower risk cases; and

   ii. potentially acting as a gatekeeper to the market for potentially higher risk AI systems (for example, by requiring them to be vetted and licensed before being released for general use).

There is a strong argument for requiring greater transparency in how AI systems deliver their output in any given case (see our answer to Question 2). Although explainability may be counter-productive in some contexts (for example, it would make no sense for an AI developer focused on fraud prevention to publish its workings to those suspected of fraud), it is clearly appropriate for AI tools operating in the employment sphere. At present, there is little incentive for developers and vendors of AI to explain how it works in layman's terms (or submit their systems to independent regulatory scrutiny). In order for employers to be able to use AI lawfully they first need to know they are actually using it and, ideally, how it works in order to assess the risk of infringing the rights of data subjects. Similarly, there is little reason for employers to try and understand it – they can simply trust the technology as there will be little risk of enforcement action being taken against them.

To manage all of this, there will need to be a proper infrastructure within existing regulators, armed with sufficient resources and a suitably skilled workforce that can understand the technology and keep up with future developments to explain measures taken to affected data subjects. It needs to be effective in regulating and providing guidance to AI developers and vendors, as well as employers. It is not clear whether the EHRC or ICO would currently be able to meet such requirements, at least not without significant assistance from several of the non-regulatory bodies listed above.

2. WHAT MEASURES COULD MAKE THE USE OF AI MORE TRANSPARENT AND EXPLAINABLE TO THE PUBLIC?

2.1 Executive Summary

The opaque nature of AI together with its application to large workforces poses major risks to employment relationships. If the UK wishes to win acceptance for the use of AI in the workplace and avoid a new Luddite reaction, then not only are more explanatory materials necessary but existing obligations to promote transparency and fairness should be strengthened and new ones considered.

2.2 'Trust and confidence': a key issue

a) AI has the power to undermine if not destroy an essential legal component of the employment relationship.

b) It is a key legal principle that in an employment relationship there must be mutual trust and confidence between the parties. Neither is allowed by law to undermine

it. It clearly poses a risk to this trust and confidence if individuals lack sufficient information to enable them to understand how their employer's decisions affect them. Indeed, employers often have a specific statutory obligation to provide that information in certain contexts.

c) The increasing use of AI-powered technology in the workplace threatens employers' ability to explain the basis of AI-assisted decisions to affected individuals:

- Technologies are complex and end users (employers) do not have the expertise to explain, in meaningful detail, how a system operates or how a decision has been reached. Some machine learning technologies are so advanced (particularly so-called 'black box' systems) that even experienced scientists cannot explain how a system has produced a particular result.

- AI-powered technology manufacturers understandably want to safeguard their commercial interests by keeping confidential certain details about how their system operates. End users (again, in this context, employers) do not have access to information which would enable them to explain how the system which they are using has produced a particular result (and, in turn, provide assurance that the system does not discriminate).

d) We question if existing legislation is adequate or whether amendments to that legislation or a new legislative regime is needed to require AI-powered technology manufacturers (and/or employers) to provide a minimum amount of information to guarantee a basic degree of transparency around decision-making which affects employees. Query if market forces are sufficient on their own to achieve this.

e) We consider the impact of AI on the employment relationship further in our answer to Question 3

2.3 Using s.1 statements?

a) s.1 Employment Rights Act 1996 mandates that the employer provides each worker with a statement of particulars of employment. It is a common misconception that the statement constitutes the contract but it does not; is merely evidence of it. It includes some provisions that are clearly part of the contract (remuneration, identity of employer) but others that may not be, such as any applicable collective agreement or details of training provided. It allows for details to be included not in the document itself but in another, readily accessible document to which it refers. This means it can cross-reference to the employer's policies.

b) It thus may be relatively simple in principle to provide that the statement references applicable AI, for example by referring to automated decisions that may be taken in respect of specified aspects of the employment. Both the concept and the detail would need careful consideration but it is potentially powerful from the employee's perspective in that it tells them personally what may affect them. At the same time, because the information may be contained in a policy, it should give the employer flexibility to change the technology or its usage and amend the policy accordingly. As with some disciplinary processes or incentive schemes,

the employer could choose to make it clear that the policy was not part of the employee's contract.

2.4 GDPR Article 22: fit for purpose?

a) The UK GDPR requires a data controller to provide basic information to a data subject about the purpose and legal basis for processing their personal data, including information about the existence of decisions made by solely automated processing (often called "automated decision-making") including at least meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject (Articles 13 and 14 UK GDPR). The information must be concise, transparent and intelligible, and in an easily accessible form using clear and plain language (Article 12 UK GDPR). Importantly, the information must be provided at the time when personal data are obtained from the data subject, or where personal data have not been obtained from the data subject, within one month from it being obtained.

b) Article 22(1) UK GDPR gives data subjects the right not to be subjected to a decision based solely on automated processing, including profiling, which produces legal effects or significantly affects the data subject. This does not apply where that automated processing is necessary for entering into or performing a contract between the data subject and a data controller under Article 22(2) UK GDPR. This is widely understood to include an employment contract.

c) When acting as a data controller, employers will likely assert there is a lawful basis for data processing by its systems of AI in the employment relationship because it is necessary for the employment contract. They might alternatively assert that the data processing by its systems of AI is necessary due to legitimate interests for itself or a third party. Importantly, the rights under Article 22 UK GDPR only apply in the latter scenario[2], but not the former.

d) Article 22 UK GDPR only applies to situations in which there is no human involvement in the data processing. However, with increasingly routine use of AI-powered technologies there is a very good chance that any human involvement will be merely cursory and have no material impact on the decision-making process which will be, in essence, entirely AI-driven[3].

e) Article 22 UK GDPR is a qualified right. Even where it applies, such as the requirement for data controllers to inform data subjects that a decision has been taken on the basis of fully automated processing[4], the current uncertainty around

---

[2] See: Article 21(1) UK GDPR.

[3] See: 'The Amazonian Era – How algorithmic systems are eroding good work' report by the Institute for the Future of Work (https://uploads-ssl.webflow.com/5f57d40eb1c2ef22d8a8ca7e/609ccc18ac8a6a30de7c5aee_IFOW%20The%20Amazonian%20Era.pdf)

[4] See: s.14(4) DPA 2018.

transparency and 'explainability' of AI systems may lead to litigation because it overlaps with existing employment law rights.

f) There have been relatively few employment law cases to date on this topic in the UK, although the topic has gained greater attention in other jurisdictions, including the EU which has sought to introduce tighter restrictions for its proposed AI Act and Platform Work Directive. We anticipate the UK will want to ensure that it keeps up with the relevant international standards to avoid adverse trade consequences.

g) In our view, it is the scope of what data processing is 'necessary' for the employment contract that seems very likely to be tested in UK litigation if clearer guidance is not provided. Each of the common employment scenarios listed above could give rise to such potential claims. It follows that the Government should consider whether further guidance should be issued about the meaning of "necessary" in Article 22(2)(a) UK GDPR, particularly whether to narrow its scope to include only those situations where there is no reasonable alternative to using automated decision-making for entering into or performing obligations under a contract of employment between a data subject and data controller.

h) ELA members have also expressed concern that routine and repetitive use can also lead to disengagement whereby the human (likely inexperienced in data science, and possibly ill-equipped to understand the system at hand) may accept a result which is produced by the system without sufficient further critical analysis of that result. Article 22 UK GDPR may therefore not reflect the commercial reality of how AI-powered technologies are being used in practice to make routine, unexplainable decisions which have far-reaching consequences for individuals in the workplace. We therefore suggest that consideration should be given to whether scope of "solely" in Article 22(1) should include automated decision-making which also involves low level or cursory human involvement and/or human involvement which is mostly administrative in nature.

2.5 Other data protection measures

a) Pursuant to Article 35 UK GDPR, employers (in their capacity as data controllers) are obliged to carry out 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". This is specifically required where automated processing, including profiling, by the data controller significantly affects the data subject. Recital 75 EU GDPR lists discrimination as a relevant risk. ICO guidance reminds data controllers to (specifically in the context of AI) address risks of bias and discrimination at an early stage.

   There is no explicit requirement to publish a DPIA under the UK GDPR. ELA suggests the Committee consider whether clarificatory guidance regarding whether DPIAs should routinely include EIAs or otherwise examine the extent to which discrimination is occurring. However, the WP29[5] recommends that data

[5] The Working Party on the Protection of Individuals with regard to the Processing of Personal Data", was an advisory body made up of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor and the European Commission.

controllers consider publishing all or part of their DPIA to help "foster trust in the controller's data processing operations and demonstrate accountability and transparency". Recital 71 EU GDPR states that automated processing should be "subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision.

b) Indeed, it may also be helpful to require organisations to seek the views of employees as part of a DPIA carried out in relation to the use of AI in the workplace. Currently an organisation has the ability to consult with data subjects or their representatives under Article 35(9) UK GDPR "*where appropriate*"; however, UK GDPR does not provide guidance for determining when it would be appropriate to do so.

2.6 Measures to strengthen workforce acceptance

a) While many employers may have a budget and specialist staff available to build knowledge about the topic, many workers will not have access to such information and resources. Given the complexity of the technology, this imbalance may lead both to meritorious claims not being brought but also unmeritorious claims being issued with those bringing them unable properly to understand their rights.

b) We therefore suggest clearer guidance on the scope of lawful processing permissible under Articles 6, 9 and 22 UK GDPR. The ICO's Employment Practices Code was published in 2011 before UK GDPR and DPA 2018 existed. While many useful recommendations continue to be relevant from Part 3 of the Code, we suggest it is updated to reflect the growth in AI that has arisen since[6]. The ICO is at the time of writing consulting on a revised code, a consultation to which ELA is contributing.

c) The ICO is currently undertaking consultation on its proposed guidance about monitoring at work (which includes sections on consultation with employees and automated decision-making) and the ECHR has produced guidance relating to AI in public services . These are welcome but unlikely to prove sufficient, even together with the other free resources currently available.

d) We also suggest the Committee consider whether:

- data controllers should be required to provide data subjects with more information; and,

- employees should be properly aware of the human oversight element in any system in advance of specific problems arising as well as having a right to sufficient information about that oversight to have redress for any such problems when they do arise.

[6] For example, at page 63 it makes clear that an impact assessment for monitoring at work can be a 'simple mental evaluation' which contradicts the requirements for processing special category data found in Schedule 1 Part 4 DPA 2018.

e) We draw the Committee's attention to existing legislation which might be amended and strengthened to achieve these objectives. This would build on a mature set of rights and obligations that overlap with requirements under UK GDPR and DPA 2018. There are two specific areas where we envisage this could be engaged.

f) **Firstly, under s.181 TULRCA 1992**. Where an employer recognises an independent trade union in respect of any class of worker, it is required to disclose to that union or to its representatives, upon request, certain information in order to enable the union to negotiate effectively. This could include information to help the employer identify and address concerns about design before the process begins, undertake reviews during the lifetime of the process and impact assessments from after the process has concluded. It could also assist the employer to conduct its DPIA in a meaningful way.

g) Secondly, under regs 4A and 7 of the Safety Representatives and Safety Committee Regulations 1977. Any recognised independent trade union may appoint a safety representative (an employee of the employer) for any workplace where it has a membership. The safety representative is entitled to require information from the employer in order to discharge their functions and consultation "in good time" about (amongst other matters) the health and safety consequences of introducing any new technologies into the workplace. This follows a general duty on employers to consult safety representatives "*with a view to the making and maintenance of arrangements which will enable [the employer] and [its] employees to co-operate effectively in promoting and developing measures to ensure that health and safety at work of the employees*."[7] The Equality Act provides for compensation for "injury to feelings" as a remedy for discrimination, so there is already some conceptual alignment in the right to compensation under Article 82 UK GDPR. It is therefore perhaps not too great a stretch therefore to infer a mandate for consultation in respect of AI where safety representatives have been appointed, recognising (as we do throughout this response) that there may be problems in defining AI and that here a relatively wide definition of AI would be required if the change were to achieve its objective.

h) The position for non-unionised workplaces is less straightforward. In respect of health and safety, similar legal requirements apply for non-unionised work groups under the Health and Safety (Consultation with Employees) Regulations 1996. However, an employer is required to provide or pay for the training of an elected representative of employee safety, whereas safety representatives appointed by a trade union will usually provide its own training. Also, the ICER 2004 places requirements on employers to inform and consult with its employees about certain matters. In practice, these rights that are rarely used, possibly because workers are unaware they exist and do not know how to enforce them.

i) In any event, we recognise these obligations place burdens on employers who may not be able to meet them without information from developers or third-party providers. To assist them, query if providers should be obliged to provide sufficient information to enable those employers to comply with their equality and data-protection obligations to provide information and consultation. The

[7] See s.2(6) Health and Safety at Work Act 1974

Committee may wish to explore the scope of liability for compensation (particularly under Chapter VIII UK GDPR and Part 6 DPA 2018) for employer data controllers and whether they would then have a right of recovery against the provider if it turned out the information was inadequate and the employer had subsequently been found liable to compensate their employees.

j) **The position of 'workers'**: Whilst as a matter of employment law the status of a "worker" is different to that of an "employee", workers and employees alike have fundamental rights to the protection of their personal data (and associated rights under the UK GDPR), and protection against unlawful discrimination in the workplace (under the Equality Act 2010). As discussed above, these are key protections relevant to the use of AI in the workplace.

However, workers have fewer statutory protections under the current employment law framework. They do not, for example, benefit from ordinary unfair dismissal protection.

In practice, workers are also more likely to work in environment in which AI systems are systematically used, and they are more likely to work in an environment in which AI systems are relied upon to produce (or feed into) processes which have significant impacts for the worker. This is borne out for example in the context of workers engaged via digital or App based platforms.

Workers are therefore both more likely to be exposed, and more vulnerable, to poorly deployed AI systems. As such, this is a group which have a particular need for protection, particularly to guard against the worst outcomes, including the risk of unlawful discrimination in the workplace.

3 HOW SHOULD DECISIONS INVOLVING AI BE REVIEWED AND SCRUTINISED IN BOTH PUBLIC AND PRIVATE SECTORS?

Are Current Options for Challenging the Use of AI Adequate and, if Not, How Can They Be Improved?

3.1 Executive Summary

- We again recommend strengthening both the roles EHRC and ICO in terms of producing relevant guidance.

- Because of the potential impact of AI on the workforce and the fact that any adverse impact is more likely to fall on workers and employees who are least able to comprehend it, we suggest consideration could be given to as to whether it is appropriate to expand existing obligations of employers to consult with trade unions and worker representatives. .

3.2 The current role of regulators in scrutinising the use of AI

a) We set out the roles of the EHRC and the ICO in our answer to Question 1. We give more detail of their specific approach to AI here.

b) Earlier this year, the EHRC announced that it has made tackling discrimination in AI a major strand of its 2022-2025 strategy[8].

i. The EHRC's functions include enforcing legal duties on public bodies to consider equality issues in all their work, and at the same time as launching its 2022-2025 strategic plan, the EHRC published guidance specifically addressing the issue of how the Public Sector Equality Duty ("**PSED**") should be applied where a public body is procuring, commissioning, building, adapting or otherwise using AI[9]. This guidance is directed at public services to ensure they take appropriate action to meet the PSED and eliminate unlawful discrimination, advance equality of opportunity and foster good relations. In particular this reminds public sector bodies that the case law (on the PSED) makes clear that it is good practice to keep a record of how equality has been considered throughout the decision-making process - often referred to as an Equality Impact Assessment, "**EIA**".

ii. The EHRC's functions include powers to conduct investigations, issue guidance and take enforcement action. In its strategic plan, the EHRC acknowledges that whilst AI has the potential to bring benefits, it also poses risks to equality and human rights, and the publication suggests that the EHRC will be looking AI in the workplace (as well as AI in public sector service delivery) including *"working with employers to make sure that using artificial intelligence…does not embed biased decision-making in practice".* The strategic plan states that, in relation to digital services and artificial intelligence, "*[the EHRC] intend[s] to intervene authoritatively to ensure that people's rights are protected online as much as they must be in real life."*

c) AI is also a priority area for the ICO, and in its strategic plan (also published earlier this year[10]) the ICO (also) emphasised concerns around discrimination in AI ("*AI-driven discrimination had become an issue that can have damaging consequences for people's lives*") seemingly with a particular focus on the workplace. Under the UK GDPR, the principle of "fairness" is understood to include expectation fairness, fairness of process and outcome fairness. Our view is that fairness is an important concept and it is right that it should be included in the principles. As explored below (under paragraph a)a.a), *Data Privacy*) this concept may be well suited to tackle some of the complexities around the use of AI. The ICO's current areas of focus include "*fairness" in AI"*[11], and the inference that we draw is that the ICO considers this principle to be central in how individuals' data is processed, particularly in this context. This is against the backdrop of the UK Government's stated intention for the UK to become a 'global

[8] EHRC - Strategic plan 2022 – 2025

[9] EHRC - Artificial intelligence in public services

[10] ICO25 strategic plan

[11] ICO – Our work on Artificial Intelligence

AI superpower' over the course of the next 10 years while still maintaining the UK's high standards for data protection[12].

3.3 Current data privacy rights & challenging the use of AI

a) Workers and employees alike have fundamental rights to the protection of their personal data. The current data privacy framework provides, to some extent, a degree of protection for these individuals in relation to the use of AI in the workplace. If personal data is used, it is subject to all the UK GDPR's principles including fairness, transparency and accountability, as we set out in our answer to Question 5.

b) However there are a number of important limitations to these rights which are particularly relevant in the context of the use of AI in the workplace, and which may constrain an employee / worker's ability to challenge the use of AI. For example:

i. Article 6 (the lawful basis of data processing) provides the legal grounds on which organisations can rely to process personal data, including in an AI context. A number of the grounds[13] (which are relevant to the employment context) are so broadly defined that there is a risk that, in practice, these may (in some cases) be treated as permitting all processing (or a very wide range or processing) within the employment relationship. As such, this may be considered to create an unacceptable degree of uncertainty around the scope of this protection.

ii. Looking at the transparency principle alone (and without consideration of the fairness principle and the obligations which arise from this principle), it appears that there is only an explicit obligation to provide an explanation of how the AI works (*"meaningful information about the logic involved, as well as the envisaged consequences of such processing for the data subject*") where the decision making falls into Article 22. (Article 13(2)(e) entails an obligation to inform individuals about the existence of decision making "*referred to in Article 22(1) and (4)*"). Article 22 has a limited scope, as we point out in our response to Question 2 and we would recommend is ripe for at least clarification if not reform.

iii. As indicated above, if personal data is used, it is subject to all the GDPR's principles including fairness, transparency and accountability. Fairness is an area the ICO is focusing on[14], and current ICO guidance[15] states that *"Part of assessing whether your use of personal data is fair is considering*

---

[12] National AI Strategy (publishing.service.gov.uk)

[13] Article 6(1)(b)&(f) UK GDPR

[14] ICO – Our work on Artificial Intelligence

[15] ICO – Explaining decisions made with AI

how it affects the interests of individuals. If an AI-assisted decision is made about someone without some form of explanation of (or information about) the decision, this may limit their autonomy and scope for self-determination. This is unlikely to be fair." As set out below, ELA suggests that this concept is well suited to tackle some of the complexities around the use of AI further guidance on how this principle should be applied in practice would be beneficial, and support transparency and trust.

3.4 The nature of the employment relationship and how this impacts the degree of scrutiny and accountability which is needed where AI is used in the workplace

a) Whilst the PSED does not apply to private sector employers, under the current legal framework, employees have a range of rights and protections which are relevant in the context of the use of AI in the workplace (and challenging that use), including statutory protection against unfair dismissal (after two years' service), rights to privacy pursuant to Article 8 ECHR[16], and the right to work without discrimination (protection afforded by the EqA). In our answer to Question 5 we address the question of whether the current legal framework (including the EqA and in particular the statutory framework for workers and those employees with less than 2 years' service) is in principle fit for purpose, and in particular, capable of tackling unfair or discriminatory uses of AI.

b) The fact that AI has been used to make (or has been a feature, or part of a process leading to) a particular decision does not alter or diminish the high standards placed upon an employer. It is well recognised that the use of AI systems in the workplace may lead to discrimination and may deepen inequality by exhibiting biases[17]. However, there are relatively few claims which have, to date, been brought by employees and workers in the Employment Tribunal. This may be attributable to a number of factors: AI is not yet as widespread in the workplace as might be thought (and without an accepted definition it is difficult to measure): a lack of awareness; or (perhaps to a greater degree), inadequate information or means to challenge the use of AI[18].

The relative lack of case law further constraints regulatory oversight, and the ability of employees to enforce their rights (the absence of case law meaning that there is an absence of practical, and accessible guidance). Whilst employees and workers will be entitled to and benefit from the data privacy rights explored above, in the employment context ELA is concerned this framework alone is not sufficient. This is both because of the unique nature of the employment relationship (explored below) which places more onerous obligations on an employer (going beyond what is currently required as a matter of data privacy

[16] In *R (Bridges) v Chief Constable of South Wales Police (Respondent) and others* [2020] EWCA Civ 1058, the court held that the use of automated facial-recognition (AFR) technology by the South Wales Police Force was in breach of Article 8 of the ECHR, the Data Protection Act 2018 and the Equality Act 2010.

[17] For example: Adams-Prassl, Binns and Kelly-Lyth, Directly Discriminatory Algorithms (2022), Modern Law Review.

[18] Page 15 of TUC report – Technology managing people – the worker experience

law) and the fact that data privacy rights cannot be enforced in the Employment Tribunal.

c) Turning to the unique nature of the employment relationship, as summarised by the co-authors of "*Technology Managing People – the legal implications"*[19]:

   i. There is an inherent power imbalance in the employment relationship. As a matter of common law, employers are required to take decisions about employees in good faith, and in a way that is lawful and rational[20] and employment contracts are subject to an implied term of mutual trust and confidence[21]. This means that actions of employers can be subject to closer scrutiny than parties to a commercial, as opposed to an employment, contract.

   ii. Employment is a personal relationship. There is a duty on the part of an employer to preserve the trust and confidence which an employee should have in them; *"this affects, or should affect, the way in which an employer normally treats his employee"*[22]. The duty of trust and confidence means that employers are, very often obliged to provide explanations to an employee where it has exercised a discretion under the contract[23]. A lack of transparency can give rise to an inference of discrimination, and so, where there is a lack of transparency related to use of AI in the workplace, an Employment Tribunal may be prepared to infer discrimination.

d) From an employee's perspective, it is not always clear when or how AI is being used. An employee may know AI is being used (for example because it is flagged in the GDPR privacy notice), however, the way the AI system works and how the employee may be affected, will often be far from transparent. For example, often an employee or worker will have no sense as to how data is feeding into more complex algorithmic management, such as work allocation or how the system used has produced a particular result. Nor is basic surrounding information is always clear, such as who is sending communications, or whether they are human or computer generated.

e) All of this creates opacity and, where concerns about discrimination, unfair or less favourable treatment are a feature, it can be difficult to properly understand or identify where processes may be falling down. The lack of the human element

---

[19] TUC report – Technology managing people – the legal implications

[20] *Braganza v BP Shipping Limited* [2015] UKSC 17.

[21] *Malik and Mahmud v Bank of Credit and Commerce International SA* [1997] UKHL 23

[22] *Keen v Commerzbank AG* [2006] EWCA Civ 1536, paragraph 44

[23] *Ibid.*

compounds the risks of marginalisation and is of itself perhaps a significant threat to what is, properly and inherently, a personal relationship[24].

f) True transparency and explainability are necessary to enable employees and workers to challenge employers if they feel they have been subject to an unfair or biased decisions or processes. If employees and workers do not understand how AI is being used, they will not understand how they can challenge such decisions and may be experience unfavourable or biased treatment without being aware of it.

g) As set out in our answer to Question 2, ELA suggests that more could and perhaps should be done to ensure employers, employees, workers and Trade Unions have sufficient information (from which to understand decisions and to assess whether AI has been used fairly, legally, and without discrimination) and that doing so would better support the current legal framework of protections, and in particular the principle of non-discrimination in the workplace. It would foster trust, and collaboration and help guard against the deployment of AI in the wrong way, leading to the worst outcomes.

3.5 The role of regulators in scrutinising the use of AI

In relation to regulatory oversight and enforcement, our suggestions are set out in our answer to Question 4.

3.6 Data privacy rights & challenging the use of AI

In relation to data privacy rights, our suggestions are set out above in our answer to Question 2

3.7 The inadequacy of the current options for employees, workers or trade unions to interrogate the use of AI in the workplace

a) AI in the workplace involves a fundamental imbalance of power between the party introducing it (the employer) and the parties subject to it (employees) in terms of information and understanding, this against the background of what is most likely to be already a fundamentally unequal relationship. Whilst as set out in our answer to this Question and Question 2, there are mechanisms available to employees to address that imbalance, they are relatively underdeveloped.

b) In the absence of a claim in the Employment Tribunal or the Courts (bringing disclosure of the relevant material in the usual manner), in practice employees and their representatives are likely to have to rely upon research, disclosure arising from other claims / litigation, or their own (personal) assessment of the outputs of the AI system. This risks encouraging litigation and a sense of unfairness, both of which are harmful in ELA's experience to good employment relations.

[24] TUC report – Technology Managing People – the legal implications

We therefore suggest:

i. Further guidance, perhaps from the EHRC, to help employers better understand their duties to provide explanations (and information) to an employee or worker where questions are asked about the use of AI in the workplace. We suggest specific further guidance to help employers and employees assess whether AI systems are compatible with Article 8 ECHR may also be beneficial;

ii. Practical and accessible routes to redress are fundamental to ensure employees and workers can challenge processes and decisions which they feel may have infringed on their rights or resulted in discrimination. Discrimination questionnaires no longer have a statutory basis . When statutory questionnaires were repealed in 2014, the Government made clear that it would remain open to an individual to ask an employer about a situation where he thinks he has suffered discrimination and, as indicated above, employers are still at risk of Tribunals drawing negative inferences from a failure to respond, and so should be encouraged to engage. In practice the experience of ELA members with questionnaires is varied. With the use of AI in the workplace, a questionnaire mechanism may encourage and support greater transparency to the rights of data subjects under Articles 12, 13, 15 and 35 UK GDPR but may not be effective without an obligation on developers and third-party providers of AI systems to provide such information to employers before the processing commences.

iii. Given both the personal nature of the employment relationship and the difficulties for any single employee to understand the technologies and their implications, we suggest the Committee considers whether there should be more support for greater involvement with workers and their representatives. Acceptance of AI may benefit from clarity as to the scope and extent of specific information and consultation rights. This is particularly important for workforces without recognised unions, and would be beneficial in promoting trust and mitigating against the risks of deploying AI in the wrong way. Under Reg 7 ICER 2004 and the statutory process for negotiating an information and consultation procedure may be initiated by either the employees or by the employer. However, in practice, this can be a protracted process and the standard I&C provisions under Reg 20 ICER 2004 lack the clarity that is needed in this context (the provisions refer to ‘any anticipatory measures envisaged’ and ‘decisions importing substantial change’). Strengthening these provisions would support greater transparency and trust. Although the threshold ‘trigger’ of a request signed by the workforce was lowered from 10% to 2% from 6 April 2020, in practice, it is still underused

4 HOW SHOULD THE USE OF AI BE REGULATED, AND WHICH BODY OR BODIES SHOULD PROVIDE REGULATORY OVERSIGHT?

4.1 Executive Summary

- Existing data protection and equality rights - and perhaps an extension of those rights - can be enforced in the workplace by the existing regulators, the ICO and EHCR.

- However, if it is decided to regulate AI as such then a new regulator will be necessary, with all the practical difficulties that entails.

- In any event, the role of guidance is key, given how fast technology moves.

4.2 How AI should be regulated

What is regulation for?

a) Before considering the precise format, or content, of any potential regulation, it is important to clarify two things:

   i. the perceived "evil" that regulation is seeking to address; and

   ii. the intended aims or purposes behind such regulation.

b) While there will likely be a number of identifiable "evils" that regulation would seek to address, for the purposes of this submission, our focus will, consistent with the other sections in this paper, be on consistency and compliance with the existing employment rights of individuals (most notably the risk of unlawful bias and/or discrimination resulting from, or facilitated by, the use of AI) and respecting the data privacy rights of individuals, including, for example, those relating to transparency and the right not to be subjected to automated decision making in circumstances where the consequences of such decisions are likely to be significant to the individual.

c) Within that context, there are a number of possible aims, or purposes, sitting behind the desire for some form of regulation of the use of AI, which are not mutually exclusive:

   i. **Encouraging compliance** by those responsible for (a) the development, and/or (b) the use, of AI, **with clear and detailed guidance** prepared, reviewed and maintained/developed by a specified regulatory body, or bodies;

   ii. **Facilitating the successful enforcement of existing actionable rights** of individuals and/or regulators by requiring a greater degree of transparency and availability of evidence of the way in which AI is used and/or the involvement or influence of AI in decision-making or processes;

   iii. **Extending existing actionable rights** of individuals and/or regulators (predominantly in the fields of employment and data protection law); and/or

   iv. **Creating new actionable rights** specifically relating to the use of AI.

d) Regulation which seeks to achieve only the latter two purposes may be less effective, or even futile, to the extent that individuals or regulators do not have the appropriate degree of information to understand if there has been any infringement of rights, or to evidence where infringements have taken place. Individuals or regulators may even lack awareness that AI has been used as part of a particular process, outcome or decision.

e) The absence of any obligation of transparency may also lead to an increasing number of unnecessarily or speculative challenges because the lack of information about how decisions are made or the use of AI itself causes individuals or regulators concern or suspicion.

Format – Regulation or Guidance?

f) The implementation of guidance alone could not realistically be said to amount to formal "regulation" for these purposes – without at least some degree of compulsion to comply, guidance could lead to unequal standards of compliance and cause more confusion/lead to greater scepticism in the eyes of the public. There remains, however, a primary question as to whether detailed guidance, backed with an appropriate degree of statutory authority on the part of a regulator to enforce compliance, may be preferable to, for example, enshrining new rights (or extending existing rights) for individuals within statute/statutory instrument.

g) The ability to enforce compliance with guidance could be granted to a regulator through an escalating series of information rights and sanctions available to them, including one or more of the following:

   i. Rights to ask questions and call for documentation of the relevant target developer/user to enable appropriate investigation as to compliance with the guidance;

   ii. Ability to seek voluntary compliance/improvement with the guidance through "informal" recommendations;

   iii. Ability to require compliance through statutory enforcement notices;

   iv. Ability formally to sanction the target developer/user through a combination of:

      (A) public censure

      (B) fines, and/or

      (C) ultimately, prohibitions from operating/using AI in the UK.

h) At least initially, it may be necessary to recognise that developers (and therefore organisations) may take time to achieve full compliance. Arguably, such an approach may fall foul of current requirements for data controllers to provide information to data subjects about automated processing under Articles 12 and 13 UK GDPR, as explained above in Q2. Consideration should be given to whether a lower sanction such as an "improvement notice" would be appropriate within a set period of time or a “grace period” within which to ensure compliance.

i) A regulator may also find it of use to have the ability to enforce a prohibition of technology for use in the UK if such technology or the developer have been sanctioned in another jurisdiction on grounds equivalent to those consistent with the approach taken in the UK.

j) This does require consideration of the extra-territorial application of any regulation. Particularly in the field of AI and technology there is the potential for competing obligations across jurisdictions, for example, where regulators in one jurisdiction heavily encourage monitoring of employees to identify potential breaches of laws but another jurisdiction considers this to be an invasive use of employees' data.

k) As stated above in our answers to Questions 2 & 3, there is already a patchwork legal framework which governs the outcome of certain uses of AI in the employment context or as part of the provision of goods and services, and the processing of personal data as part of the use of AI. There is a need to look at existing underlying rights and identify whether any amendments are needed to secure a greater degree of protection for individuals without the wholesale introduction of new actionable rights.

l) If new AI related actionable rights which individuals can enforce are considered, this may result in additional complications. For example, this raises questions as to whether the employment tribunal or court system would be the appropriate forum. Additionally, AI related actionable rights requires consideration of whether class actions or representative actions should be permissible.

Who should be regulated?

m) It is important for the focus of any regulations not simply to be on the "client to public" relationship (by public in this context, we mean the end user of that tool, often the employee). Jumping over the "provider to client" relationship and skipping straight to the "client to public" relationship would also render regulation less effective.

n) In the absence of any obligations on developers or other third-party providers, ELA members have seen a reluctance from providers to volunteer appropriate transparent information to client users, which then in turn limits what can be provided to end users (in this context, employees).

o) This may be because of a tension between transparency and intellectual property issues – many developers or service providers consider the inner-workings of the algorithm to be proprietary information. This may also be because sales or marketing staff at the provider do not themselves have sufficient information to explain how the AI tool works or how decisions are made, which in turn may be because the market is not demanding it.

p) Manufacturers, developers and sellers of AI and AI-related tools should have the primary obligation, to be enforced by a regulator, of ensuring and demonstrating that the tool or software complies with regulation and sufficiently details guidance, including requirements on transparency on how the tool operates.

q) This will require consideration of the following issues:

    i. What does transparency mean, particularly if technology uses deep machine learning or neural networks?

    ii. Does transparency differ depending on the audience? For example, is there any obligation to provide information as to the formula of any AI or algorithmic

tool? Or must either individuals using the technology within an organisation or an end user at the client be provided with information which they can understand in layman's terms?

iii. Should transparency mean information which, for example, workers' representatives can use to understand wider patterns or information which individual end users can use to understand about specific impact on them?

iv. Should there be a requirement in any AI tool for the tool itself to be able to, in accessible terms, explain how a decision is made?

r) One possibility is for AI tools developed by third-party providers have a "Kitemark" or some other standard approach to demonstrate that the technology has created in accordance with the concept of "AI ethics by design" and, for example, tested on appropriate datasets to avoid or mitigate the risk of bias.

s) Users of the technology will still need to have some responsibility and a degree of accountability on them, for example, to carry out their own diligence before using or deploying AI tools.

Regulation supplemented by guidance

t) To regulate the multitude of scenarios in which AI is used and the wide spectrum of organisations which make use of AI, regulation needs to be supplemented by guidance which is clear and thought through in detail, including consulting with key stakeholders and experts. Guidance needs to deal with difficult and sophisticated examples, rather than straightforward "easy" cases. It is imperative that guidance is maintained and supplemented as technology evolves.

u) All guidance needs to be backed by a clear statement of what will happen when the relevant organisation or entity (i.e. the developer or the user organisation, as applicable) is found to be in breach of that guidance.

v) Further guidance is needed in any event to assist individuals and organisations understand how the current legal framework applies to the use of AI. To give some examples:

i. If there is to be new regulation specific to AI, there will need to be a clear definition of what AI is. We identify some of the problems with is in our response to Question 1. In any event, some degree of standardisation of a definition of AI would be helpful to give individuals and organisations greater certainty as to what is and what is not, subject to the regulation (perhaps with technologies that are similar being excused to comply on a more voluntary "best practice" basis).

ii. The EHRC has produced guidance for the public sector on the use of AI in the context of public sector equality duties under the Equality Act 2010. The private sector could also benefit from guidance from the EHRC on the application of the Equality Act 2010 to the employment sphere and the provision of goods and services.

iii. Specific guidance would be helpful on the need or otherwise (and content, if needed) for generally accepted standards for organisations to adopt in statements of ethical principles or as part of ESG requirements for listed or regulated companies. Currently these are novel and not yet explored fully in this context (save for sophisticated technology companies or those holding very large amounts of data), sector specific or voluntary.

iv. Guidance needs to make a clear distinction between AI tools that facilitate human decision making (for example, tools which sort data but do not exclude any data from human review) and tools have the effect of making a decision with significant impacts for individuals (even if early in the process).

Which Body or Bodies should regulate the use of AI?

4.3 The suggestion that the EHRC, the ICO, the FCA, PRA and other regulators such as the CMA would all be given powers to regulate the use of AI is problematic. Using multiple regulators to govern the use of AI is likely to give rise to inconsistency and a waste of resources through duplication.

4.4 No current regulator has the appropriate funding or resources and none have the full skillset required. For example, the ICO is the regulator with the current greatest experience in the regulation of the processing of data using technology. However, if an existing body such as the ICO is appointed for the regulator of AI tools, it would require significant investment. The ICO is significantly under resourced to deal with the issues already within its remit. Having said that, even if sufficiently funded, a single brand new regulator would lack experience.

4.5 We note that many regulators have expertise within their spheres which may be valuable. One option would be for a single regulator to be a joint venture staffed with appropriately skilled representatives from each existing regulator seconded in, plus technology experts, data analysts etc. This would require investment, training and clear lines of sight to existing regulators with free-flowing channels of information.

4.6 All that said, in the workplace, ELA does not consider a single regulator to be an absolute necessity. The EHRC and the ICO have different remits covering different aspects of AI as it affects employees. If each is properly resourced and both work together to resolve any competing policy objectives, then alongside the regulatory and legislative changes we suggest there is no compelling case to merge their activities in a single organisation for the benefit of employers and employees.

5 TO WHAT EXTENT IS THE LEGAL FRAMEWORK FOR THE USE OF AI, ESPECIALLY IN MAKING DECISIONS, FIT FOR PURPOSE?

Is More Legislation or Better Guidance Required?

5.1 Executive summary

- We repeat, in the workplace there is no framework as such for the use of AI. We suggest both more legislation and better guidance, building on existing protections for data and equality. See our response to Questions 1-4.

- We also urge better enforcement. Regulators need more powers to promote fairness and transparency. Individuals need that fairness and transparency to identify issues and secure redress.

5.2 We describe the current framework, the roles of regulators and the gaps in our previous answers. In responding to this question, we focus on enforcement. Synthesising some our earlier points by way of introduction:

a) **Lack of overall enforcement body** - as of now, there is no regulatory body that has overall supervision of the use of AI. Query if one is necessary in the workplace given the ICO and EHRC cover the main employment issues of data and equality, but if it is thought better to regulate AI specifically as opposed to regulating its impacts then we suggest a specific regulator would be necessary.

b) **Lack of enforcement power -** it is also unclear to what extent existing bodies have powers of enforcement against parties other than the purported decision maker e.g. the employer. In most cases, it will be the vendor of the AI system that has the clearest understanding of the AI development process and arguably should bear some of the responsibility for any adverse impact caused by the software. Query if this should be directly through regulation or through contract, with regulation perhaps facilitating claims by employers against vendors if the product has exposed them to regulatory sanction.

c) **Reliance on enforcement by individuals** - the other way in which complaints about AI software can potentially be raised relies on an individual employee bringing an employment law (unfair dismissal/detriment) or indirect discrimination claim in the employment tribunal or bringing a (more costly) data privacy claim in the civil courts. These claims are, however, rarely brought in the UK, despite the acceptance of potential bias in algorithms and well publicised examples of adverse effect (see above). Why is this? The prospect of litigation is already daunting for individual employees but they are even more so in AI related cases where there is often a lack of transparency and explainability, often referred to as the "black box" problem. If the employer does not (or cannot or will not) explain how the algorithm works, on what grounds can the applicant/employee show that their suspicions of discrimination are founded?

Given the gaps identified above, ELA hopes that a combination of legislative clarification and guidance can enable employees and employers to better understand the implications of use of AI, and to challenge use which breaches data protection and discrimination laws.

We have set out below a list of potential changes that the Committee could consider although we make no recommendations on any particular course of action.

5.3 How to improve enforcement.

We suggest that the following proposals be evaluated by the Committee:

a) Creating a Statutory Code of Practice for explainability and in particular how Article 22(3) UK GDPR should be satisfied (see our answers to Questions 2 & 3).

b) Considering whether to create a right for individuals to request a discrimination questionnaire (similar to the old statutory discrimination questionnaire) to obtain information about an AI-based decision or outcome, including statistical analysis of disparate impact conducted by the employer (see our answer to Question 4).

c) Creating an obligation on obligations for vendors / creators of AI, to provide disclosure of their statistical analysis of disparate impact, either as part of a questionnaire type process or through the employment tribunal proceedings.

d) Promoting the requirement for data controllers to conduct DPIAs when processing data through automated processes and that there are wide circumstances when it would be appropriate to consult with data subjects or their representatives under Article 35(9) UK GDPR.

e) Guidance from the Government or EHRC on inferences to be drawn or burden of proof under section 136 Equality Act 2010 to pass to the employer where they fail to comply with any transparency obligations.

f) Considering the establishment of a regulatory body with specific responsibility for AI (similar to approach of EU AI Directive).

g) Increasing awareness of AI obligations and individual rights through information campaigns.

6 WHAT LESSONS, IF ANY, CAN THE UK LEARN FROM OTHER COUNTRIES ON AI GOVERNANCE?

6.1 There have been a number of legislative initiatives around the world responding to multiple use cases. There have also been further proposals and plentiful instances of guidance. Numerous themes can be identified which may offer some lessons to be learned for the UK. Typical concerns emerge from the employment perspective, particularly bias and, to a lesser extent, more general workforce impact and management, although we consider that in any assessment of legislative framework the latter should not be the poor cousin of bias concerns. Pragmatically, there is also the issue that the UK will have to consider consistency of approach from the perspective of not disadvantaging UK business accessing other markets. The following commentary covers proposed legislation and amendments to already existing laws.

6.2 A number of initiatives include outright prohibitions on use cases that they deem unacceptable. A good example of this is the proposed EU AI Act which identifies four levels of risk (unacceptable, high, limited and minimal), before regulating on a risk-based approach, imposing a requirement of an iterative risk management system. When a high-risk AI system is developed it needs to undergo a conformity assessment to ensure compliance with AI requirements to be later registered in stand-alone AI systems in an EU database and, finally, issued with a signed declaration of conformity. Notably, the accredited AI system should use so-called "CE marking" which invites consideration whether a kite-marking system would be beneficial in the UK. Others, such as the proposed amendments to Californian legislation, take an approach which seeks to narrow the permitted purposes for which AI may be used that do not harm workers' physical or mental health, their personal safety and well-being.

6.3 Some legislative initiatives are proposing that regulation is only effectively triggered where there is sole reliance on AI. For example, in Illinois, employers who solely rely on the AI analysis of video interviews to determine which applicants receive in-person interviews are required to annually report certain data related to race and ethnicity of applicants. Similarly, proposed legislation in Quebec requires companies that make decisions using personal information that are based exclusively on AI to inform the affected individuals. We would regard this precondition for the application of legislation as inherently flawed and narrowing the scope of specific protections. The limitations are apparent in Article 22 of the UK GDPR where protection of individuals only arises in case of solely automated processing. In the AI context, any factor requiring human oversight should not defeat the further application of any legislative protection.

6.4 There have also been attempts to suggest that AI can (only) be used in a discriminatory manner where it is "necessary" for screening purposes (e.g. proposed amendments to Californian legislation). This does not sit well with the duty, at the very least of employers, to meet the obligation to make reasonable adjustments to those who are disabled and who suffer from a substantial disadvantage. Washington DC suggested permissibility, if linked to an affirmative action programme, but that does not easily translate to the UK where there are only very limited exceptions for positive discrimination.

6.5 There is also the question of how different jurisdictions are addressing the challenge as to which party to attribute liability – the question arises as to how it should be apportioned between the provider of AI and the user. The proposed amendments to current Californian law, interestingly, suggest joint and several liability where there is unlawful use. By contrast, the proposed EU AI Act seeks to differentiate between provider and user which can give rise to potentially difficult questions. For example, where an employer-user seeks to adapt the original AI, does it make the employer a provider and, therefore, relieves the original provider of any liability. Any legislation or regulation needs to address this distinction and, where the dividing lines may well prove blurred in practice, incentivise vendors and providers to ensure AI is lawful. In this context it is worth noting the approach of the EU's proposed AI Liability Directive which aims to give victims of damage caused by AI equivalent protection to victims of damage caused by products in general. This includes significant powers to order disclosure, and a rebuttable presumption of a causal link in the event in the case of the fault of the defendant and the output or failure of output of the AI system at issue.

6.6 Requiring impact assessments before implementation is a common theme (e.g. in California and the EU). In some instances, it is anticipated that this will be undertaken by the business, elsewhere by an independent assessor, and, in turn, with assessment by a relevant labour agency. The proposed amendments to Californian legislation suggest the list of potential risks to be assessed and requires methodology and mitigation to be described rather than prescribing actual content. Additionally, proposed amendments to Californian law suggest that summaries of such impact assessments should be published on the employer's website. There is an opportunity here for regulators to create a model approach, building on the experience of DPIA conducted to date. We would encourage a proportionate and consistent approach to avoid disincentivising compliance. The proposed EU AI Act requires a provider of "High Risk AI" (e.g. using AI to determine access to vocational training or in employment, management of workers and access to self-employment) to ensure conformity with established principles by a relevant authority to ensure, broadly, responsible and lawful usage of AI by way of an accreditation process.

6.7 Elsewhere (e.g. Canada and California) there are proposals to conduct regular audits either by the employer or third parties. Such an audit would demonstrate the risks and mitigation measures taken in respect of the systems with high impact and compliance measures and relevant safeguards adopted that would reveal any contraventions. Given the systemic nature of AI risk, pre-emptive assessment, as well as after the event remediation, has clear attractions. Interestingly, in December 2021, New York passed a pioneering law requiring employers to audit their AI tools for bias before these can be used for recruitment, hiring or promotion. The law will take effect on January 1, 2023. The role of post implementation audits will also be critical, given the evolving nature of AI through machine learning and adaptation.

6.8 Various initiatives require transparency by way of providing notification about the use of AI to job candidates and employees (New York, Illinois, California, Spain). However, this raises the problematic point as to whether there can validly be informed consent and/or a fair waiver of any rights by a job candidate or an employee. This point has already been debated in the context of individual consent to data processing under the GDPR, and whether an employee's consent is ever freely given. That said, Maryland has passed a law requiring employers to obtain a job applicant's consent ahead of using facial recognition tools in the recruitment process. An option worth

further exploration is the extent to which providing an employee with an option to opt-out would amount to a viable solution (as prescribed under the laws of Colorado and Connecticut and proposed amendments to Californian legislation) If so, such a proposition would require further protection from detrimental treatment on the grounds of any opt-out right being exercised.

6.9 The role of employee representatives should also be considered. The German legislation, under the Works Council Modernisation Act, gives works councils' considerable powers with regard to co-determination rights. This requires the councils' engagement at the very outset, before any introduction of AI in the workplace. The proposed amendments to Californian legislation also anticipates an enlarged role for representatives and prescribes that such bodies are engaged in consultation, affording protection against any retaliation for having raised concerns or issues. In Spain, the New Act on Digital Rights requires that workers' representatives are given information about monitoring tools used that affect decision-making and access to continuing employment, including the rules and instructions on which algorithms are based. (For completeness, Spain has also introduced specific legislation applicable to delivery riders, presuming employment status where shifts are allocated by AI).

6.10 The density of the UK's union membership and patterns of recognition means that, in many instances, there will not be an established collective bargaining mechanism for prior engagement with representatives and related disclosure obligations. The UK is, of course, fully familiar with election of representatives for redundancy purposes or business transfers but these are when specific instances arise. This raises interesting questions as to when workforce impact might be contemplated during the course of AI design as well as implementation. That said, given the general perspective of inequality of bargaining power between employer and employee, already noted in the context of consent above, this does invite further scrutiny of the nature of any regulatory engagement, the confidence that can be placed in self-regulation, and, then, the activist nature of any enforcement regime. We suggest in our response to Question 2 how the UK's existing consultation regimes may be enhanced.

6.11 Where a regulator's role has been anticipated in the legislation's design, this anticipates a sole labour agency. This raises questions as to the UK's cross-sectoral approach with multiple regulators. This could prove problematic both in terms of capacity building and resourcing the relevant expertise as well as ensuring consistency of application of standards and enforcement. To date, we have seen both the ICO and the EHRC as the lead regulators. In this context, joint guidance would be appropriate. The Equal Employment Opportunity Commission ("EEOC") has spearheaded this initiative in the US, with a particular focus on ensuring no discrimination contrary to US Federal law by encouraging the adoption of "Promising Practices". As a general recommendation, multiple differing sets of guidance should be avoided. In terms of ensuring compliance, there is clearly a significant role for training, both within regulators and without.

6.12 Finally, there is the related issue of remedy and enforcement. To ensure consistency, there should not be variable routes to remedy dependent on the choice of regulator. Additionally, enforcement regimes clearly need to amount to a sufficient deterrent. Fines by way of a fixed penalty per violation (e.g. the proposed amendments to Californian legislation) or by reference to turnover comparable to competition law (e.g.

the proposed EU AI Act) have been proposed. Required remediation should also include broader steps, as seen with data protection legislation approached, such as correction or deletion.

ELA Working Party Members:

Jonathan Chamberlain	Gowling WLG (UK) LLP (Chair)
Jessica Bass	Curzon Green
Jamie Cameron	Burges Salmon LLP
Jonathan Exten-Wright	DLA Piper
Dominic Holmes	Taylor Vinters
Deborah Margolis	GQ Littler
Sian McKinley	Herbert Smith Freehills
James Morrison	Doyle Clayton
Martin Pratt	Ince
Bruce Robin	Unison
Julia Wilson	Baker McKenzie
Hannah Wright	Bates Wells

ELA Contact Person:

James Jeynes
Head of Operations

jamesj@elaweb.org.uk
01895256972