

DISPATCH NO. 39 – EUROPEAN UNION

THE AI ACT AND ALGORITHMIC MANAGEMENT

Aislinn Kelly-Lyth[†]

In April 2018, just before the GDPR came into force,¹ the European Commission adopted a Communication on Artificial Intelligence (AI).² In it, the Commission declared that the EU could “lead the way in developing and using AI for good and for all.”³ Three years later, the Commission published a proposal for a Regulation laying down rules on artificial intelligence (the proposed ‘AI Act’).⁴ The proposal is now progressing through the early stages of legislative consideration.⁵ This Dispatch outlines the relevance of the Act for the employment context, including its objects, scope, and possible impacts. It also highlights some key areas of concern: the lack of external supervision over compliance assessments; the inadequacy of the proposal’s transparency provisions; and the potential deregulatory effects of the Act at the domestic level.

THE ROAD TO REGULATION

To understand the importance of the AI Act in the employment sphere, one must first consider the Commission’s objectives in this space. The 2018 Communication provided the foundation for a series of important milestones

[†] Researcher, University of Oxford, aislinn.kelly-lyth@law.ox.ac.uk. I acknowledge funding from the European Research Council under the European Union’s Horizon 2020 research and innovation program (grant agreement No 947806).

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter ‘GDPR’) came into force on 25 May 2018, see art. 99.

2. *Communication from the Commission to the European Parliament, The European Council, The Council, The European Economic and Social Committee and the Committee of the Regions, Artificial Intelligence for Europe*, COM (2018) 237 final (June 26, 2018).

3. *Id.*

4. *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, COM (2021) 206 final (April 22, 2021) (hereinafter ‘AI Act’).

5. In Parliament, the file has been provisionally assigned to the Committee on Internal Market and Consumer Protection. In Council, negotiations have begun between Member States. See *Artificial Intelligence Act*, COD (2021) 0106.

on the road to the proposal,⁶ the most significant of which was the Commission's White Paper on Artificial Intelligence, published in February 2020.⁷ Both the 2018 Communication and the 2020 White Paper identified a need to address the impact of AI on the labor market. However, a close reading of the documents reveals a shift in understanding about the nature of that impact.

Although the 2018 Communication stated that "AI is changing the nature of work," the Commission's concerns were that tasks would be automated, and that more jobs would require technological skills.⁸ The Commission thus identified three primary goals: (i) upskilling Europeans to develop "basic digital skills"; (ii) helping workers "in jobs which are likely to... disappear"; and (iii) training more AI specialists.⁹

By 2020, the Commission's focus had changed: its White Paper recognized that "[b]eyond upskilling, workers and employers [who are still in employment] are directly affected by the design and use of AI systems in the workplace."¹⁰ The use of AI in "situations impacting workers' rights" was therefore provided in the White Paper as an example of a high-risk AI application for which stricter legal requirements should be adopted.¹¹ In short, between 2018 and 2020, the Commission recognized that AI not only threatens to extinguish certain jobs—it is *already transforming in-work experiences* across the socio-economic spectrum by enabling the automation of functions traditionally performed by managers.

In March 2021, the Commission explained that AI systems "are often applied to guide recruitment, monitor workloads, define remuneration rates, manage careers or increase efficiency of processes."¹² It is now common for job applications to be rejected without ever being considered by a human;¹³ for employees' keystrokes to be tracked;¹⁴ and for voice analysis software to

6. In June 2018, the High Level Expert Group on AI (AIHLEG) was set up. In April 2019, the Group presented Ethics Guidelines for Trustworthy Artificial Intelligence. For a full list of milestones, see European Commission, *A European approach to artificial intelligence*, <https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence>.

7. *White Paper on Artificial Intelligence – A European Approach to Excellence and Trust*, COM (2020) 65 final (Feb. 2, 2020).

8. COM (2018) 237 final, *supra* note 2.

9. *Id.*

10. COM (2020) 65 final, *supra* note 7, at 7.

11. *Id.* at 18.

12. *The European Pillar of Social Rights Action Plan*, at 19, COM (2021) 102 final (Mar. 3, 2021).

13. S. Buranyi, 'Dehumanising, Impenetrable, Frustrating': the Grim Reality of Job Hunting in the Age of AI, *The Guardian* (Mar. 4, 2018), <https://www.theguardian.com/inequality/2018/mar/04/dehumanising-impenetrable-frustrating-the-grim-reality-of-job-hunting-in-the-age-of-ai>.

14. Sandy Milne, *Bosses Turn to 'Tattleware' to Keep Tabs on Employees Working From Home*, *The Guardian* (Sept. 5, 2021), <https://www.theguardian.com/us-news/2021/sep/05/covid-coronavirus-work-home-office-surveillance>.

be deployed at call centers to analyze workers' tone and speed.¹⁵ This phenomenon of technology-enabled worker monitoring and control—often termed ‘algorithmic management’—is what the AI Act, insofar as it regulates labor, seeks to address.

Algorithmic management tools can have their benefits. Participatory shift scheduling tools can enable employees to exert greater control over their scheduling patterns, for example.¹⁶ But there are also clear risks to fundamental rights: as well as posing obvious privacy concerns, there is evidence that some algorithmic management tools exhibit discriminatory tendencies, for example.¹⁷

SCOPE OF THE ACT

At first blush, the proposal is strikingly wide. The Act's definition of ‘AI’ is extremely broad: a program which uses statistics to generate recommendations, for example, is ‘AI’ under the proposed Act.¹⁸ Not all forms of AI are treated equally by the proposal, however. The bulk of the Act's provisions apply only to two sub-categories of software. First, AI systems which are held to pose an “unacceptable risk” are presumptively prohibited.¹⁹ Secondly, AI systems which are deemed to pose a “high risk” are subject to a specified set of requirements.²⁰ Beyond these two categories, the Act has little bite. Certain hard-to-spot forms of AI, such as deepfakes, are to be rendered more observable,²¹ and voluntary codes of conduct are encouraged in other cases.²² But the most pressing questions for employers—and for employee representatives—will all relate to the rules on presumptively prohibited and high-risk AI.

PROHIBITED AI

The list of unacceptable (and therefore prohibited) AI is short: four systems are *prima facie* banned under Article 5, and only one of these stands

15. Tom Simonite, *This Call May Be Monitored for Tone and Emotion*, *Wired* (19 Mar. 19, 2020), <https://www.wired.com/story/this-call-may-be-monitored-for-tone-and-emotion/>; see also <https://cogito.corp.com/>.

16. Jarno Turunen, Kati Karhula, Annina Ropponen, Aki Koskinen, Tarja Hakola, Sampsa Puttonen, Kari Hämäläinen, Jaakko Pehkonen, & Mikko Härmä, *The Effects of Using Participatory Working Time Scheduling Software on Sickness Absence: A Difference-in-differences Study*, 112: 103716 *Int'l J. of Nursing Stud.* (2020).

17. Alina Köchling and Marius Claus Wehner, *Discriminated by an Algorithm: a Systematic Review of Discrimination and Fairness by Algorithmic Decision-making in the Context of HR Recruitment and HR Development*, 13 *Bus. Rsch.* 795 (2020).

18. See AI Act, *supra* note 4, art. 3(1).

19. AI Act, *supra* note 4, at art. 5.

20. The requirements for high-risk AI are set out at Title III, Chapter 2 of the Act.

21. AI Act, *supra* note 4, at art. 53.

22. AI Act, *supra* note 4, at Title IX.

out as potentially relevant in the employment context.²³ This is the prohibition on systems that “deploy[] subliminal techniques beyond a person’s consciousness” in order to “materially distort” their behavior in a manner that is likely to cause “physical or psychological harm.”²⁴

In practice, very few algorithmic management tools will fall within this definition, not least because the harmful manipulation must be intentional.²⁵ The example provided by the Commission, which Veale and Zuiderveen Borgesius aptly describe as “border[ing] on the fantastical,”²⁶ is “[a]n inaudible sound [played] in truck drivers’ cabins to push them to drive longer than healthy and safe [where] AI is used to find the frequency maximising this effect on drivers.”²⁷ Such a situation not only seems highly improbable—it would likely be unlawful under current EU legislation.²⁸ In short, in its current form, the prohibition on “unacceptable” AI is unlikely to have much impact in the employment sphere.

RULES ON HIGH-RISK AI

We turn, therefore, to the second category of AI which the Act seeks to regulate: systems which pose a “high risk”.²⁹ The Act adopts a list-based approach to identify such systems,³⁰ and does so through a two-stage categorization: Annex III identifies eight “areas” into which high risk systems may fall, and within each high-risk “area” is a sub-list of use cases. Only AI systems intended to be used for these specified purposes are subject

23. AI Act, art. 5(b) relates to exploitation of vulnerability of particular groups, such as children or persons with disabilities. This is unlikely to be relevant in the employment context. Art. 5(c) relates to the sale and deployment of systems used by public authorities. Art. 5(d) relates to the use of ‘real-time’ biometric identification systems for the purpose of law enforcement.

24. AI Act, *supra* note 4, at art. 5(a).

25. The deployment of the subliminal techniques must be ‘in order to’ distort the person’s behavior, *Id.*

26. Michael Veale & Frederik Zuiderveen Borgesius, *Demystifying the Draft EU Artificial Intelligence Act*, 22(4) *Comput. L. Rev. Int’l* 4, (2021) (forthcoming, pre-print version 1.2).

27. Gabriele Mazzini, *A European Strategy for Artificial Intelligence* (2nd ELLIS Workshop in Human-Centric Machine Learning) (May 10, 2021), <https://www.youtube.com/watch?v=OZtuVKWqhI0&t=10346s&ab_channel=ELLISHCML>, circa 2:52:00.

28. See Directive 2002/15/EC of the European Parliament and of the Council of 11 March 2002 on the Organisation of the Working Time of Persons Performing Mobile Road Transport Activities, 2002 O.J. (L 080), art. 5.

29. These are systems that pose ‘significant risks to the health and safety or fundamental rights of persons’ by virtue of their (intended) use: *Explanatory Memorandum to COM (2021) 206 – Harmonised final*, p. 3. *Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, COM (2021) 206 final (April 22, 2021).

30. AI Act, art. 6 classifies two forms of AI as ‘high-risk’: systems already regulated by EU product safety legislation listed at Annex II; and any systems listed at Annex III. The former category of high-risk AI relates, for example, to software used in toys and medical devices. Changes to the regulation of this category of technology are unlikely to have major impacts in the employment sector. Regulation of the latter category, namely of the systems listed under Annex III, is more likely to be significant.

to the rules applicable to “high-risk” AI. The Commission is empowered to update the sub-lists, but cannot alter the eight overarching “areas”.³¹

One of the eight high-risk areas is “employment, workers management, and access to self-employment”.³² Two use cases appear in the sub-list for this area: (i) systems used for recruitment; and (ii) systems used for promotion and termination of contracts for work, for allocating tasks, and for monitoring and evaluating workers’ behavior.³³ In other words, the Act identifies employment as a high-risk area, and specifically pinpoints algorithmic management tools as requiring further regulation.

The question, then, is what that regulation entails. The “requirements for high-risk AI systems” are set out in Chapter 2 of the Act, and essentially amount to certain design criteria, implemented at the pre-market stage. For example, Article 9 stipulates that a “risk management system shall be established,” which shall consist of a “continuous iterative process” that identifies, evaluates, and mitigates “risks”, while Article 10 requires that data sets used for high-risk AI “shall be subject to appropriate data governance and management practices,” including “examination in view of possible biases.”³⁴ The providers are further required to provide the aforementioned “instructions of use,” which must (*inter alia*) identify the technology’s “intended purpose,” its “accuracy,” and any “known or foreseeable circumstance” which may lead to health and safety or fundamental rights risks.³⁵

As such, most of the obligations fall to the AI *provider* (the person/body that develops or markets the AI), rather than its *user* (the person/body who uses the system).³⁶ Translating this into the employment context, an employer who purchases a people analytics tool which professes to measure workers’ productivity will face relatively few new obligations.³⁷ She must use the tool in accordance with its instructions of use, and must monitor its operation on the basis of those instructions.³⁸ She must also ensure that any data she inputs is “relevant,” and must keep any logs automatically generated by the system.³⁹ But it is the vendor who must design the technologies to comply with the Act’s standards, and must demonstrate such compliance by

31. AI Act, *supra* note 4, at art. 7.

32. AI Act, *supra* note 4, at Annex III, ¶ 4.

33. *Id.*

34. AI Act, *supra* note 4, at art. 12.

35. AI Act, *supra* note 4, at art. 13(3).

36. AI Act, *supra* note 4, at art. 3(2), (4).

37. Note that the employer will continue to be subject to existing relevant regulation (see AI Act, art. 29(2)). This includes, in particular, the European Convention on Human Rights, art. 8; and the GDPR.

38. AI Act, *supra* note 4, at art. 29(1), 29(4).

39. AI Act, *supra* note 4, at art. 29(3), 29(5).

reference to a set of technical documentation “drawn up before [the] system is placed on the market”.⁴⁰

This division of obligations is almost a mirror image of the GDPR. In the algorithmic management context, the employer will usually be the data controller for GDPR purposes, thus shouldering the lion's share of responsibility for data protection compliance.⁴¹ If the algorithm vendor has a role, it will be as processor (entailing fewer obligations) or joint controller (in which case the obligations are shared).⁴² In the AI Act, the roles are reversed, with the vendor bearing a far greater burden than the employer.

How would this new division of duties affect algorithmically managed employees? In theory, the imposition of rights-protective obligations on algorithm vendors is a step in the right direction: employers' data protection obligations must not be watered down, but vendors who design and understand their products should also pull their weight in mitigating rights impacts.⁴³ The question, though, is whether the obligations offer sufficient protection against accidental fundamental rights infringements, let alone rogue AI use. In this respect, the proposal is far from perfect.

MARKING ONE'S OWN HOMEWORK

First, one of the Act's core proposals is that every “high-risk” AI system placed on the market should be accompanied by a “conformity assessment” confirming that the requisite AI standards have been met.⁴⁴ Conformity assessments are a concept borrowed from product safety legislation: readers may be familiar with the ‘CE’ markings which appear on products ranging from children's toys to travel adaptors, indicating that these items have met EU legislative standards.⁴⁵

Whether it is right to adopt a product safety approach for AI systems remains open to debate. For present purposes, however, it is worth noting that

40. AI Act, *supra* note 4, at art. 11.

41. The employer will usually determine the ‘purposes and means’ of processing and will therefore be the data controller (GDPR, *supra* note 1, at art. 4(7)). It will generally be the employer who will decide to automate a managerial function, and they will select the vendor and algorithmic product which fulfils that function. *See generally* European Data Protection Board, *Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR*, version 2.0 adopted on 7 July 2021.

42. If the vendor only processes the employees' personal data on behalf of the employer (but does not determine the ‘purposes and means’ of processing), then they will be a processor (GDPR, *supra* note 1, at art. 4(8)). If the employer and vendor jointly determine the ‘purposes and means’, they will be joint controllers, *see* European Data Protection Board, *Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR*, version 2.0 adopted on 7 July 2021 § 3.

43. For an example of a vendor setting out its interpretation of its own and the purchasing employer's GDPR duties, *see* Microsoft, *Data-protection considerations when using Workplace Analytics* (30 August 2021) <https://docs.microsoft.com/en-us/workplace-analytics/privacy/data-protection-considerations>.

44. AI Act, *supra* note 4, at Ch. 4 & 5.

45. *See* Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the Safety of Toys, 2009 O.J. (L 170); Directive 2011/65/EU of the European Parliament and of the Council of 8 June 2011 on the Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment, 2011 O.J. (L 174); and Directive 2014/35/EU of the European Parliament and of the Council

the Act envisages that conformity assessments for algorithmic management tools will be *self-assessments*.⁴⁶ In other words, algorithm vendors will certify their *own compliance* with the Act. Self-assessment is not unusual in EU product safety law,⁴⁷ and may be adequate if requirements are clearly defined – but here AI providers will be certifying (for example) that data sets used to train the algorithms are sufficiently “relevant”, “representative”, and “free of errors”.⁴⁸ In light of such vague stipulations, it is possible that self-assessments could become rubber stamps.⁴⁹

The Act does propose external compliance checks for certain forms of AI (few of which are relevant for our purposes),⁵⁰ and a Recital implies that external certification *could* be expanded to other cases after the “initial phase of application” of the Act.⁵¹ However, a clearer and binding timeline for expanding external certification to all high-risk AI, including algorithmic management, would be a significant improvement.

TRANSPARENCY FOR WHOM?

One of the most significant aspects of the GDPR was the unprecedented transparency it afforded to individual data subjects.⁵² While hardly a panacea, these provisions have, for example, enabled gig economy workers to demand access to some information about algorithmic decisions affecting them.⁵³ The AI Act, on the other hand, does little to provide algorithmically managed workers with access to information about their employers’ automated decisions. Article 13 declares that an “appropriate type and degree of

of 26 February 2014 on the Harmonisation of the Laws of the Member States Relating to the Making Available on the Market of Electrical Equipment Designed for Use within Certain Voltage Limits, 2014 O.J. (L 96). For more information on CE marking, see https://europa.eu/youreurope/business/product-requirements/labels-markings/ce-marking/index_en.htm. Provision is made in the Act for a CE marking, see AI Act, *supra* note 4, at arts. 19, 49. In fact, much of the proposal is drawn from the EU’s product safety framework: see Veale & Borgesius, *supra* note 26, at 3.

46. AI Act, *supra* note 4, at arts. 43(2), 48.

47. The EU maintains a list of regulated products, specifying whether external assessment by a notified body is necessary for each (or whether self-assessment is adequate): https://ec.europa.eu/growth/single-market/ce-marking/manufacturers_en.

48. AI Act, *supra* note 4, at art. 10(3); Recital 44.

49. For discussion on the inadequacy of self-assessment, see Nathalie Smuha, Emma Ahmed-Rengersb Adam Harkens, Wenlong Li, James MacLaren, Riccardo Pisellif and Karen Yeung, *How the EU Can Achieve Trustworthy AI: A Response to the European Commission’s Proposal for an Artificial Intelligence Act* (LEADS Lab @University of Birmingham, 5 August 2021), pp. 37-40.

50. Products already regulated by EU product safety legislation listed at Annex II are subject to external assessment: AI Act, *supra* note 4, at art. 43(3). In addition, biometric systems will be subject to external certification unless the provider has applied (not yet established) harmonized standards: AI Act, *supra* note 4, at art. 43(1); Annex III ¶ 1. Biometric systems could be used by some employers as part of their monitoring activities.

51. AI Act, *supra* note 4, Recital 64.

52. See GDPR, *supra* note 1, at arts. 5(1)(a), 13, 14.

53. C/13/687315 / HA RK 20-207 *Uber drivers v Uber* ECLI:NL:RBAMS:2021:1020, ¶¶ 4.46, 4.52 (Neth.); C/13/689705 / HA RK 20-258 *Ola drivers v Ola Cabs* ECLI:NL:RBAMS:2021:1019 ¶¶ 4.25, 4.46, 4.52, 4.62.

transparency shall be ensured,” but this is limited to enabling *users* (in the labor context, employers) to “interpret the system’s output and use it appropriately.”⁵⁴ The absence of transparency for *impacted individuals* is part of a broader and fundamental problem with the proposal: unlike the GDPR, the AI Act completely fails to reference AI ‘subjects’ and their representatives.⁵⁵

Given the absence of any reference to impacted individuals, from the employee perspective the most promising provision under the current proposal is Article 60. This provides for a publicly accessible “database” containing information about high-risk AI systems, including the ‘instructions for use’ for high-risk algorithmic management tools.⁵⁶ As above, the instructions for use must include information about the characteristics, capabilities and limitations of the AI system.⁵⁷ Such information might enable trade unions and other social partners to assess at a high level whether algorithmic management tools on the market could contravene employee rights.

The Act should, however, do much more to empower AI system subjects, including by ensuring that workers can access information to assert their employment, equality, and data protection law rights. For example, workers could be granted access to the “technical documentation” underpinning algorithmic management tools used by their employers.⁵⁸ The technical documentation will contain information such as “the key design choices including the rationale and assumptions made” and the system’s “degrees of accuracy for specific persons or groups of persons.”⁵⁹ Access to this documentation might empower workers to bring litigation challenging unlawful algorithmic decision-making—a route which is very difficult under existing laws.⁶⁰

A CEILING, NOT A FLOOR

Finally, perhaps the most concerning aspect of the AI Act is its potential *deregulatory* effect in some jurisdictions. The Act is a positive harmonization measure, which means that EU Member States would be prohibited from

54. AI Act, *supra* note 4, at art. 13(1).

55. This ‘blind spot’ has been criticized by the European Data Protection Board and European Data Protection Supervisor, see *Joint Opinion 5/2021 on the Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)*, ¶ 18 (June 18, 2021). There are numerous references to ‘data subjects’ in the GDPR.

56. AI Act, *supra* note 4, Annex VIII, ¶ 11.

57. AI Act, *supra* note 4, at art. 15(3).

58. AI Act, *supra* note 4, at art. 11.

59. AI Act, *supra* note 4, Annex IV.

60. See Aislinn Kelly-Lyth, *Challenging Biased Hiring Algorithms*, Oxford J. of Legal Stud. (2021).

maintaining any laws incompatible with the standards laid down by the Act.⁶¹ The proposal thus threatens to prevent domestic legislatures from maintaining higher standards on AI deployment, including in the employment context.⁶² This is particularly concerning when one considers that some jurisdictions currently limit the use of workplace monitoring tools.⁶³ If the Act prohibits States from providing worker with protection but fails to introduce similar Union-level rules, that would be a retrograde step indeed.

It is not necessary for the Act to prevent progressive action on worker rights. The GDPR, for example, expressly provides that Member States may “provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees’ personal data”⁶⁴—thus setting a floor, rather than a ceiling. It is imperative that a similar provision be included in the AI Act in order to prevent dangerous deregulatory effects.

CONCLUSION

The proposed AI Act represents a clear step forward in terms of regulating AI, and is likely to have impacts beyond the EU.⁶⁵ If adopted, it will force algorithm vendors to take clear risk mitigation measures before marketing certain tools, with potential benefits for those affected by their deployment. However, several key issues remain to be worked out if the Act is to have a positive impact for algorithmically managed employees. In particular, external certification—rather than self-certification—should be imposed for all high-risk AI; employees affected by AI tools should be guaranteed access to detailed information about those tools; and a clear carve-out should be created for EU Member States to set higher standards on AI use in the workplace. This legislative proposal represents a critical opportunity to shape the development of workplace technology—and it is crucial that we get it right.

61. See Explanatory Memorandum, *supra* note 29, at 6, explaining that the legal basis for the proposal is Art 114 of the Treaty on the Functioning of the European Union (TFEU). This Article empowers the EU to harmonize national laws in order to ensure free movement of goods, services, capital and people within the internal market.

62. The material scope of the AI Act (and thus the ‘occupied field’) is extremely broad due to the Act’s definition of ‘AI’, see AI Act, *supra* note 4, at art. 3(1). For further discussion on harmonization and pre-emption, see Veale & Borgesius, *supra* note 26, at 20-23.

63. See Valerio De Stefano, *The EU Proposed Regulation on AI: a Threat to Labour Protection?*, Wolters Kluwer (Apr. 16, 2021), <http://regulatingforglobalization.com/2021/04/16/the-eu-proposed-regulation-on-ai-a-threat-to-labour-protection/>.

64. GDPR, *supra* note 1, at art. 88.

65. The territorial scope of the Act is broad: see AI Act, *supra* note 4, at art. 2(1).