Written Evidence Submitted by Liberty

(GAI0081)

ABOUT LIBERTY

Liberty is an independent membership organisation. We challenge injustice, defend freedom and campaign to make sure everyone in the UK is treated fairly. We are campaigners, lawyers and policy experts who work together to protect rights and hold the powerful to account.

Liberty provides policy responses to Government consultations on all issues which have implications for human rights and civil liberties. We also submit evidence to Select Committees, inquiries and other policy fora, and undertake independent, funded research.

CONTENTS

INTRODUCTION

1. Liberty welcomes the opportunity to respond to the call for evidence on governance of artificial intelligence (AI).[1] Noting that AI broadly refers to the field of science that aims to replicate human intelligence abilities in computers, for the purposes of this response we confine our comments to automated decision-making (ADM, also known as algorithm-based, or algorithmic, decision making). We understand ADM to mean the utilisation of algorithms to automate various tasks, and which make, supplement, or play a part in decision making.

QUESTION 1

How effective is current governance of AI in the UK? What are the current strengths and weakness of current arrangements, including for research?

2. Liberty is aware of the Government's plans to undertake a review of the AI Governance landscape.[2] According to the National AI Strategy this will include looking at current regulation and legislation, regulator expertise and capacity and the institutional landscape including standards and assurance bodies. Nevertheless, we disagree with the Government's approach of ensuring the regulatory regime "facilitates innovation" while at the same time "[protects] people and our fundamental values." Taking the facilitation of innovation as its starting point undermines the importance of human rights and seeks to put it on an equal footing of what is inherently a business-led model of experimentation. It is particularly revealing that when the Government set out to detail the content of their much awaited, and delayed White Paper on AI Governance, the development of a "*pro-innovation national* position on governing and regulating AI" appears to have been prioritised over and above "human rights, democratic principles, and the rule of law" which itself was deemed relevant only to shaping *international* and not UK frameworks, norms and standards for governing AI.[3]

3. Rather than prioritise innovation, or even hold innovation and fundamental rights in equal esteem, the primary consideration for the Government must be to ensure that the governance of ADM (especially the legal framework governing use of biometric data in particular) is compatible with the rights of individuals; the key questions being whether the laws and policies are adequately prescribed by law, necessary, and a proportionate means of achieving a legitimate aim. A further primary consideration must be whether the use, collection or retention of data, or wider

[1] Science and Technology Committee, AI Governance Call for Evidence. Available at: https://committees.parliament.uk/work/6986/governance-of-artificial-intelligence-ai/
[2] National AI Strategy. Available at: https://www.gov.uk/government/publications/national-ai-strategy
[3] National AI Strategy, p.61.

policy context behind the use of ADM (e.g. how and on whom the police decide to deploy tech), will result in unlawful discrimination, as well as exacerbate and entrench systemic oppression.

4. The use of technologies in the justice system provides an illustrative example of the inadequacy of the UK's AI governance regime (or rather, lack thereof). While only making up one part of many of ADM's possible uses (welfare provision and public health are other significant examples), there is no consolidated or clear framework in this area. Governance of technologies in the justice system sits across the Human Rights Act 1998 (HRA), Data Protection Act 2018 (DPA), Equality Act 2010 (EA), public administration, police common law powers to 'prevent and detect crime,' the Protection of Freedoms Act 2012, law enforcement bodies' own published policies, a raft of guidance, regulation and other guidelines, and has over 30 public bodies, initiatives, and programmes playing a governance function.[4] This demonstrates the scale of governance challenges, and speaks to the complexity, lack of cohesion, and confusion around who and what play key roles in oversight, responsibility and accountability.

5. When the House of Lords Select Committee on Justice and Home Affairs sought to find a neat and coordinated 'family tree' of the organisations involved in the governance of new technologies for the application of the law, Professor Paul Taylor, National Policing Chief Scientific Advisor, told them that "it may be more of a family bush."[5] The fact that a high-level policing advisor attests to the level of confusion and disorientation of this field speaks volumes. As explained by one respondent to the Committee's call for evidence, this is nothing short of a 'public failure' which could "lead to not just operational defects or ineffeciencies, but miscarriages of justice," which, without "accountability for errors and misuse […] may leave people open to dangers for which no person can be identified as responsible."[6]

6. In the policing and criminal justice context, the miscarriages of justice arising from errors are obvious, ranging from wrongful imprisonment to police monitoring, surveillance and harassment. But it is worth noting the life-changing consequences that can also happen in other, seemingly more innocuous circumstances. In 2020, after the coronavirus pandemic caused A-Level examinations to be cancelled, the Office of Qualifications and Examinations Regulation (Ofqual) decided to use an algorithm to determine pupils' final grades. The algorithm considered three data

[4] House of Lords Justice and Home Affairs Committee, Technology Rules? The Advent of New Technologies in the Justice System. Available at: https://publications.parliament.uk/pa/ld5802/ldselect/ldjusthom/180/180.pdf
[5] House of Lords Justice and Home Affairs Committee, Technology Rules? The Advent of New Technologies in the Justice System, Q98 Professor Paul Taylor, p.21.
[6] House of Lords Justice and Home Affairs Committee, Technology Rules? The Advent of New Technologies in the Justice System, written evidence from Professor Nigel Harvey and Tobias Harvey, p.14.

inputs: the historical grade distribution of schools from the three previous years (2017-2019); the rank of each student within their own school for a particular subject, based on a teacher's predicted grade (referred to as the 'Centre-Assessed Grade'); and the previous exam results for a student per subject. Specifically, it looked at the historical distribution of grades within a school, and then decided a student's grade on the basis of their ranking in the context of that distribution.

7. The algorithm led almost 40% of students to receive grades lower than they had anticipated,[7] prompting significant outcry and legal action, particularly around issues of unfairness. Lord Falconer and then shadow education secretary Kate Green noted that the formula for standardising grades was in breach of the overarching objectives under which Ofqual was established by the Apprenticeships, Skills, Children and Learning Act 2009, which required that the grading system "(a) give a reliable indication of achievement, and (b) indicate a consistent level of attainment (including over time) between comparable assessments."[8] They also said that the algorithm was inherently unfair and risked breaching the Equality Act.[9]

8. The use of the A-levels algorithm had severe consequences for pupils across the country. But it also had a particular disproportionate impact on the most marginalised students, particularly due to the distinction between young people enrolled in private schools (who make up just 7% of the population) as compared to state schools – in which marginalised groups are overrepresented (for instance an important indicator of poverty is eligibility for free school meals, the axis of yet another pandemic scandal).[10] Significantly, students were not initially given a right of appeal. Ofqual was eventually forced to make a u-turn, withdrawing the algorithm in a matter of days after multiple groups threatened legal action, and scrapping the grades in favour of teachers' predicted results.[11] UCAS revealed that 15,000 pupils originally rejected by their first-choice university obtained the grades needed to meet their offer after the u-turn, with 90% of them aiming to study at top-tier universities.[12]

---

[7] Bedingfield, W., *Everything that went wrong with the botched A-Levels algorithm*, Wired, 19 August 2020, available at: https://www.wired.co.uk/article/alevel-exam-algorithm

[8] Para 377, Explanatory notes to the Apprenticeships, Skills, Children and Learning Act 2009

[9] Elgot, J. and Adams, R., *Ofqual exam results algorithm was unlawful, says Labour*, The Guardian, 19 Aug 2020, available at: https://www.theguardian.com/education/2020/aug/19/ofqual-exam-results-algorithm-was-unlawful-says-labour

[10] Poverty also disproportionately impacts children and young people growing up in BAME families. See National Education Union, *Child poverty: the facts*, 03 May 2021, available at: https://neu.org.uk/child-poverty-facts. See also the 'free school meal scandal': https://www.theguardian.com/education/2021/jan/20/rashford-demands-a-meal-a-day-for-all-school-pupils-in-need

[11] Kolkman, D., *"F**k the algorithm"?: What the world can learn from the UK's A-level grading fiasco*, LSE, 26 August 2020, available at: https://blogs.lse.ac.uk/impactofsocialsciences/2020/08/26/fk-the-algorithm-what-the-world-can-learn-from-the-uks-a-level-grading-fiasco/

[12] Adams, R et al., *Ofqual ignored exams warning a month ago amid minister's pressure*, 19 August 2020, available at: https://www.theguardian.com/politics/2020/aug/19/ofqual-was-warned-a-month-ago-that-exams-algorithm-was-volatile

9. According to the HRA, any interference with rights must be (amongst other things) "in accordance with the law." As such, there is an explicit requirement for underlying legislative safeguards to satisfy the principle. Further, caselaw has explained that as part of this requirement, there needs to be safeguards in law which make the use of the power foreseeable and accessible – the public must know how the power will be used, and how discretion is limited. With AI Governance scattered as it is, it is simply insufficient that for technology which is so intrusive, there exists no tech-specific statutory framework.

10. Considering this fragmented framework, and the organisational confusion on the part of public bodies about what framework applies in their use of ADM, we are perturbed by the Government's dismissal of attempts by the Home Affairs and Justice Committee to meaningfully address governance concerns (including, but not limited to, the establishment of a proper governance structure with the ability to carry out regular inspections, a strong legal framework, and legislation introduced to establish clear principles). Significantly, the Government suggested that issues could be clarified by the courts, an approach which will become significantly more difficult to do should, as discussed in Questions 3 and 5 the Government's dangerous plans to repeal and replace the Human Rights Act, as well as the Retained EU Law Bill[13] and Data Protection and Digital Information Bill, come into fruition.

11. There are significant dangers to an approach which relies on the Courts to set governance standards, and we are already starting from the wrong footing if the assumption is that something is lawful, until it is proven otherwise by legal challenge. This is at complete odds with the rule of law: it is the role of Government, with Parliamentary scrutiny, to determine governance, set standards, and empower public bodies to comply with them. While the Courts can hold back the tide on particular instances of use, it is difficult to bring legal challenges, not to mention the difficulties of finding a client, attaining funding in an environment of cuts to legal aid,[14] limitations on what arguments may be run, and wider Government plans to limit Judicial Review.[15]

12. In Liberty's experience, even after a successful legal challenge (such as after the Court of Appeal's *Bridges* judgment which ruled live facial recognition (LFR) technology unlawful and breached privacy rights, data protection and equality laws), there is no guarantee that public bodies will change their approach. Liberty is aware

[13] Public Law Project second reading briefing on the Retauned EU Law (Revocation and Reform) Bill, October 2023, https://publiclawproject.org.uk/content/uploads/2022/10/Second-Reading-Commons-Briefing-REUL-Bill-final.pdf
[14] Amnesty International, *Cuts that Hurt: the impact of legal aid cuts in England on access to justice*, https://research.thelegaleducationfoundation.org/wp-content/uploads/2017/11/aiuk_legal_aid_report.pdf
[15] Liberty's Briefing on the Judicial Review and Courts Bill for House of Commons Report Stage, January 2022 https://www.libertyhumanrights.org.uk/wp-content/uploads/2019/12/Libertys-briefing-on-the-Judicial-Review-and-Courts-Bill-report-stage-HoC-Jan-22.pdf

of operational deployments of LFR undertaken by the Metropolitan Police, and we understand that it is still in use by South Wales Police. Further, police forces are scoping and have procured other facial recognition technologies such as retrospective facial recognition,[16] facial recognition watches,[17] and mobile phone/hand-held facial recognition devices.[18]

QUESTION 2

What measures could make the use of AI more transparent and explainable to the public?

13. While we acknowledge that the underlying intention of this question is to ensure that AI systems are "more transparent and explainable to the public," we are worried that this framing ignores wider questions about how AI systems may entrench structural oppression and works from a likely baseless assumption that wholly mitigating problems in AI systems is even possible, and specifically, possible simply through making the systems more transparent and explainable. This is akin to attempts made to address 'bias' in AI – a fundamentally 'technocentric' approach that focuses on technical debiasing that obscures broader questions about the development and context-specific implementation of AI and related technologies, and structural inequality and discrimination. Transparency is a vital step in AI governance, but one that, once the operation and impact of AI is made transparent, may – and should in many situations – lead to the rejection of AI altogether from public life.

14. In addition to making AI more transparent and explainable to the public then, we must substantively assess the underlying policy objectives for which ADM systems are being deployed, as well how such systems are being deployed. To understand the purpose of an AI system, and to consider its human rights compatibility we should follow the human rights principles of necessity and proportionality at every stage of the ADM system's design and operation, including the decision to collect certain kinds of data, the processes through which this data is collected, processed, and shared, the design of the algorithm, and the effects it has on public decision-making.

---

[16] Emma Woollacott, *London's Met Police Buying Retrospective Facial Recognition Technology,* Forbes. Available at: https://www.forbes.com/sites/emmawoollacott/2021/09/28/londons-met-police-buying-retrospective-facial-recognition-technology/

[17] Nicola Kelly, *Facial recognition smartwatches to be used to monitor foreign offenders in UK,* 5 Aug 2022. Available at: https://www.theguardian.com/politics/2022/aug/05/facial-recognition-smartwatches-to-be-used-to-monitor-foreign-offenders-in-uk

[18] Demi Roberts, *Police in Wales to be first in UK to use handheld face recognition technology to identify wanted suspects.* 9 Dec 2021. Available at: https://www.walesonline.co.uk/news/wales-news/police-wales-first-uk-use-22401241

15. Similarly, we should consider proportionality by taking into consideration the full ADM system. For example, it has been revealed that gig economy companies have previously collected data about workers using disproportionate surveillance tactics, including monitoring when workers have not logged in to make themselves available for work, or flagging workers who fail to accept enough of the work being offered to them on a given platform as fraudulent, thereby effectively coercing them to work longer hours. Even if this data feeds into an ADM system designed for the innocuous purpose of allocating work, the extent and kind of surveillance levied against workers would be enough for us to consider the ADM system potentially rights-violative. The way that data is collected can also be scrutinised under the data protection legislation and the Public Sector Equality Duty, for example if it is found to disproportionately affect people with a protected characteristic.[19]

16. Given the many risks inherent in ADM systems, it is crucial that – at the very least – they are proven to be effective at their stated purposes on the basis of evidence involving a wide range of stakeholders, objectively researched, and taking into consideration the wider context of systemic oppression that the system is operating in. All too often, new technologies are introduced into a vacuum of evidence, in the context of an active public relations campaign by a manufacturer that promises to save a public body money in the long-term. By the time there is an evidence base, use has been normalised, and such normalisation forecloses the ability for a wider societal and Parliament-led conversation about whether it is appropriate or desirable to use the AI system in the first place. There may also arise circular logics, whereby public bodies seek to justify the mass collection of personal data on the basis that decision-making systems (including ADM systems) require greater amounts (and better quality) of intelligence; in turn, public bodies may seek to justify the creation of more extensive and unaccountable decision-making systems on the basis that there is simply too much data being collected to be processed without some degree of automation, even when these decisions have effects on our human rights.

17. If an ADM system is not effective, then it is unlikely to be necessary or proportionate, but crucially, we also note that effectiveness is not the best or full measure. A fundamentally rights-violative decision-making system – for example, one that is based on fundamentally rights-violative policy – can never be rehabilitated on the basis of efficiency or effectiveness.

---

[19] For example, the way that data was collected and processed under the Gangs Matrix was considered by the Information Commissioner as potentially involving issues of discrimination and equality of opportunity (though she did not consider these issues in depth) as well as breaching data protection law. See: ICO, Enforcement notice (MPS Gangs Matrix), 13 November 2018, available at: https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/about-us/gangs-violence-matrix/ico-enforcement-notice.pdf

18. An analogous example of this can be found in debates over facial recognition technology (FRT). FRT is a demonstrative example of a technology that is inherently rights-violative (being a technology that will always involve the mass processing of thousands' biometric data and shift the power away from individuals to the state), and for which transparency and explainability is an inadequate solution. Currently, police must put up signs warning the public of their use of facial recognition. However, this is not a sufficient marker of transparency, and people have been detained by police for trying to divert themselves away from the cameras, of which is their right.[20] Moreover, it should not be left to the individual to notice (small) signs and take steps to avoid and protect themselves from oppressive state surveillance as they go about their everyday lives; this itself is a further violation of the right to free expression. The tech just should not be used.

19. A significant barrier to transparency in the context of ADM systems is the extent of the involvement of the private sector in their development, and in some cases, their implementation (in collaboration with the public sector). Just as with public bodies, in cases where there is a public-private partnership, or the development of the algorithm has been outsourced, it is necessary to consider the private company's stated purpose in developing the system. While a profit motive on the part of a private company or a cost-saving motive on the part of a local council is not necessarily problematic, it should form part of the evaluation of the necessity of the ADM in the round.

20. Crucially, unlike public bodies, the private sector is not bound by the same safeguards – such as the Public Sector Equality Duty within the Equality Act 2010 (EA) – and is able to shield itself from criticisms regarding transparency behind the veil of 'commercial sensitivity'. In addition to considering the private company's purpose, AI governance itself must cover the private as well as public sphere, and be regulated to the same, if not a higher standard. This could include strict procurement rules – for example that private companies need to release certain information to the end user/public, and independent auditing of AI systems. Further, civil society organisations have advocated for a mandatory national register of ADM systems which is accessible and explainable to the public. The accomplishment of Equality Impact Assessments and wider Human Rights Assessments could also be mandatory, as well as their publication.

21. Overall, it is important that underlying questions about ADM's human rights compatibility are addressed, to inform issues to do with transparency and

[20] Lizzie Dearden, *Police stop people from covering their faces from facial recognition camera then fine man £90 after he protested,* The Independent, 31 Jan 2019. Available at: https://www.independent.co.uk/news/uk/crime/facial-recognition-cameras-technology-london-trial-met-police-face-cover-man-fined-a8756936.html

explainability. These are two principles which are, of course, fundamental to human rights assessments, but we must not work from the assumption that the harms arise only from the lack thereof of these things.

QUESTION 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?

22. As already addressed, Liberty is alert to this Government's attempts to stop people from holding power – in this case, opaque and unfair decision-making on the part of State bodies and private organisations – to account, alongside a wider agenda of making itself untouchable. As such, current options for challenging the use of AI are not adequate, and are at risk of being undermined further.

23. Currently, ADM systems are subject to some specific regulation via the Data Protection Act 2018 (DPA) and UK GDPR. The DPA provides for a right not to be subject to solely ADM that produces an "adverse legal effect" on, or "significantly affects", the data subject - unless that decision is "required or authorised by law"[21] (or other limited exceptions). Any such significant decision authorised by law must be "subject to safeguards for the data subject's rights, freedoms and legitimate interests", including: the right to be informed by the data controller that such a decision was made and the right, within one month, to request a reconsideration or a retaking of the decision "that is not based solely on automated processing". A further month is allotted for reconsideration or retaking and for the data subject to be informed of the outcome.[22] The vast majority of the exemptions contained in the DPA, allowing data processors to set aside a person's data protection rights for broadly-defined purposes such as public protection and crime, do not apply to ADM.[23]

24. The DPA thus allows for significant decisions to be made by sole ADM so long as authorised by law or accompanied by safeguards (in other words, sole ADM is permittable under wide-ranging conditions). During scrutiny of the DPA, Liberty recommended that Parliamentarians support an amendment that would have protected individuals from solely ADM engaging their rights under the Human Rights Act 1998. This would have been a significant, if bare minimum, safeguard; however, the amendment did not succeed.

---

[21] Data Protection Act 2018, Section 49, https://www.legislation.gov.uk/ukgpa/2018/12/pdfs/ukgpa_20180012_en.pdf.
[22] *bid.*, Section 14(5).
[23] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/?q=article+4

25. Further, the DPA allows for significant decisions to be made by ADM *without* being authorised by law or accompanied by safeguards, so long as a human is in the loop (in other words, partial ADM is always permittable). Liberty has advocated for the protections under Article 22 UK GDPR to be extended more widely in order to refute the presumption that partial ADM poses less risks that sole automation by virtue of its human involvement. On the contrary, we believe similar risks arise from all forms of ADM and caution against putting too high a premium on human oversight as a robust safeguard. This is because of the risk of 'automation bias', whereby individuals are for various reasons liable to simply giving a 'rubber stamp' of approval to automated decisions, rather than considering the automated decision as one factor. For example, in a situation where an individual police officer is required to make a decision as to whether to arrest a suspect, it is conceivable that they would defer to the ADM system and engage in an arrest for fear of going against what is purportedly 'better' intelligence (even if it may not be). In turn, "human users who are provided with advice by machines will often become increasingly reliant on and uncritical of this advice with time."This is a very real threat: low knowledge levels regarding AI among end users (in part because private manufacturers restrict information) coupled with time restraints and a lack of empowerment to meaningfully challenge ADM decisions, mean that what is meant to be a decision-*assisting* tool becomes a decision-*making* tool in practice. The narrow definition of solely ADM under the DPA also means that many ADM systems, including the facial recognition technology now being rolled out by the Metropolitan police, may not be caught by the DPA because they arguably include meaningful human involvement. **Liberty would encourage clarification and expansion of the meaning of sole ADM to extend to instances where there is human involvement, and would seek to dismantle the distinction between sole and partial ADM altogether.**

26. The UK is undertaking its process of changing its data protection regime post-Brexit via the Data Protection and Digital Information Bill (currently making its way through Parliament). This Bill provides another pertinent example of proposals recommended in the name of governance being a euphemism for reducing legal protections for individuals and their data. The REUL Bill further risks eroding essential data protection laws in the UK, by giving the Government broad powers to amend laws falling within the category of 'retained EU law' and allow currently unidentified swathes of these laws to disappear at the end of 2023 unless specifically 'saved' by a minister.[24] The Government has also indicated that it plans to proceed with the repeal and replacement of the Human Rights Act, which will undermine rights protections including individuals' data and privacy rights as well as their right to freedom of expression – essential safeguards that ensure that AI systems can be

[24] https://publiclawproject.org.uk/content/uploads/2022/10/Second-Reading-Commons-Briefing-REUL-Bill-final.pdf

held to account and that would need to form the basis of any meaningful discussion on AI governance more broadly.

27. Not only do these changes risk endangering human rights, they also risk threatening the data adequacy agreement that the UK currently maintains with the EU, which would have wide-ranging impacts, including on UK businesses.[25] This further calls into question the practical feasibility and effectiveness of the Government's so-called 'pro-innovation' approach.

28. Notwithstanding our concerns about the UK GDPR, legislation around automated decision-making which governs when decisions about people can be made using algorithms and AI, and what rights those people then have to object, ask for human review, or seek redress (Article 22) does provide a stronger floor of protection than the proposals made to change it in the Data Protection and Digital Information Bill. While the Bill hasn't removed controls over automated decision-making altogether, we have significant concerns about the ways in which Article 22 is rewritten. As identified by the organisation, Connected by Data, the Bill

    a. Is not sufficient to tackle harms arising from automated decision-making, including the use of unfair and discriminatory algorithms that widen inequalities,
    b. [Flips] the original regulation in Article 22 on its head: instead of automated decision-making being prohibited except for when it's safe, it's now allowed except for under what are judged to be risky circumstances,
    c. Doesn't make the distinction between data subjects (those who the data is about) and decision subjects (those who are affected by automated decision making),
    d. Puts particular protections in place around the use of special category data in algorithms only (recent EU case law has found that special category data can sometimes be derived from non-special category data - such as deriving someone's sexuality from their spouse's name, or race from the area where they live),
    e. Gives the Secretary of State the power to determine whether a given decision does or doesn't have a 'significant effect', and
    f. Allows organisations to get around many of the protections the Bill does provide around automated decision making through a minimal inclusion of a person in the decision making process (something which we have already explored, and drawn attention to the shortcomings of, above).[26]

[25] https://ico.org.uk/media/about-the-ico/consultation-responses/4020181/ico-response-to-moj-human-rights-act-reform-consultation.pdf
[26] Connected by Data, *What should change in the Data Protection and Digital Information Bill*, 29 Sept 2022. Available at: https://connectedbydata.org/events/2022-09-29-data-protection-digital-information-bill-civil-society-event

QUESTION 4

How should the use of AI be regulated, and which body or bodies should provide regulatory oversight?

29. The rapid advances in the field of artificial intelligence and machine learning represent a huge shift in the relationship between the individual and the state. For example, the prevalence of data collection that is required to enable ADM systems to work has ushered in widespread surveillance technologies, whose purpose is to lay bare the intimate details of people's everyday lives.

30. Since algorithmic models are based on data, the content of that data – and the way it is collected and processed – is significant. Marginalised communities can be subject to discrimination via the dual threat of being both under and overrepresented. As an example of the former, a range of studies have revealed the biases inherent in facial recognition technology due to the reliance of training data on white, straight, cis-gender men.[27] Less explored, however, are the risks to marginalised communities of being *over*represented in data. Wealth and social privilege shield certain populations, for example, those who opt for private healthcare or who do not access benefits, from tools of societal control and surveillance. As Virginia Eubanks details when speaking of the "invisible spider web" of ADM, "many of us in the professional middle class only brush against it briefly, up where the holes in the web are wider and fewer of the strands are activated. We may have to pause a moment to extricate ourselves from its gummy grasp, but its impacts don't linger."[28] In contrast, poverty and race, through proxy indicators such as access to public services and residential postcodes (or in some cases, even names),[29] attract over-policing and hyper-surveillance, which then proceeds to feed the data mined by the algorithm to produce the desired outputs. For example, an ADM system used to flag a child in need of protective services in the US, was based on data gathered from public service providers (such as public drug support services), rather than private data (such as private rehabilitation centres).[30] In other

---

[27] Buolamwini et al (2018), *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Proceedings of Machine Learning Research, 2018 Conference on Fairness, Accountability, and Transparency

[28] Virginia Eubanks. *Automated Inequality: how high-tech tools profile, punish and police the poor* (2018).

[29] In April 2018, it was revealed that police data fed into the HART system was supplemented using an Experian dataset called "Mosaic", produced through profiling each of the 50 million adults in the UK. Mosaic profiles and classifies people into spurious groups – for example, a *"crowded kaleidoscope"* is a low-income*, "multi-cultural"* family working *"jobs with high turnover"* and living in *"cramped houses"* and *"overcrowded flats"*. Mosaic even links names to stereotypes: for example, people called Stacey are likely to fall under *"Families with Needs"* who receive "a range of benefits". Terrence and Denise are *"Low Income Workers"* who have *"few qualifications"* and are *"heavy TV viewers"*. See: Big Brother Watch, *Police use Experian Marketing Data for AI Custody Decisions* [Press release], 6 April 2018, available at: https://bigbrotherwatch.org.uk/all-media/police-use-experian-marketing-data-for-ai-custody-decisions

[30] Virginia Eubanks. *Automated Inequality: how high-tech tools profile, punish and police the poor* (2018).

words, the more you interact with the State, the more data points are likely to exist about you that are accessible by public bodies, and the greater the State's ability becomes to track you across society.

31. The police's deployment of new technologies that seek to analyse and predict crime outcomes and identify and profile people are also having a seismic impact on the way laws are being and will continue to be enforced, magnifiying existing inequalities and oppression. A prime example is the Gangs Matrix, a Metropolitan Police Service database containing personal information of people perceived to be in a gang or likely to commit violence. In 2018 the Information Commissioner published an enforcement notice which ruled that it had been consistently breaching data protection laws since its creation.[31] Research found that 15% of people on the Matrix were children (some as young as 12) and 78% were Black males.[32] Reasons for being placed on the Matrix were opaque and could result in criminalisation and difficulties accessing public services – children and young people on the Matrix faced the risk of over-policing, school exclusion, eviction, and in some cases being stripped of welfare benefits, being taken into care, or even deportation. Following a legal challenge focusing on the racial disproportionality of the database, the MPS was forced to conceded that their operation of the Matrix was unlawful. It has now finally agreed to radically overhaul the database and to remove more than a thousand names from it.[33]

32. In addition to the implications that come from privacy, data protection and human rights perspectives, there arises the larger issue surrounding the lack of democratic engagement with whether we should, as a society, have these technologies in the first place. In turn, the question must be asked of whether the public can have such a discussion, if they are not well-informed, and the Government is not proactively engaging them in this debate. By questioning whether technologies can be used correctly and reliably within a regime of regulation and oversight, we have already foreclosed the wider question of whether these technologies should be used at all.

33. While there should be bare minimum and stringent safeguards to ensure accountability and transparency, there will also be various cases where ADM should be banned entirely, including when ADM systems involve the use of data which flow from oppressive practices in the first place (such as racist policing). **In summary, Liberty does not believe that regulation can fix the harms of ADM.**

---

[31] https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/about-us/gangs-violence-matrix/ico-enforcement-notice.pdf

[32] Amnesty International (2018) *Trapped in the Matrix: Secrecy, stigma, and bias in the Met's Gangs Database*

[33] Liberty (11 November 2022) 'Met to overhaul 'Racist' Gangs Matrix after landmark legal challenge'

QUESTION 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?

34. There is no comprehensive statutory legal framework for regulating the creation or use of ADM systems in the UK, and current arrangements provide a mere floor of protection. We are highly concerned by the Government's agenda to weaken data protection and privacy rights, as well as dismantle the overarching human rights frameworks, repealing and replacing the Human Rights Act (HRA) with the Bill of Rights (or more accurately, the Rights Removal Bill).

35. Crucial to the protection of data rights is Article 8 of the European Convention on Human Rights (ECHR) (incorporated in the UK by the HRA). Through its dangerous plans to introduce the Rights Removal Bill the Government will drastically curtail the crucial rights that the HRA protects and which act as a fundamental backstop for the protection of data rights and automated decision-making more widely. **The UK Government must reject the Bill of Rights Bill, and retain our Human Rights Act.**[34]

36. Data protection and privacy rights are also deeply interconnected with, and essential tools for enforcing, a host of other rights, not least our rights to freedom of expression and freedom of assembly and association. Crucially, data protection and privacy rights can be one of the most important – and in some cases, the only – way that people can stand up to untransparent and unfair decision-making by public and private bodies, because they are sometimes the only way to find out if one has even been subjected to such a decision. Data protection and privacy rights have enabled individuals to challenge the unfair withholding of benefits,[35] discriminatory policing and targeting,[36] expansive and intrusive surveillance,[37] racist immigration visa-streaming algorithms,[38] and wage theft in the context of precarious 'gig' economy employment[39] - and much, much more. Given the increasing use of technology in the

---

[34] Liberty's briefing on the Bill of Rights Bill for Second Reading in the House of Commons, July 2022. Available at: https://www.libertyhumanrights.org.uk/wp-content/uploads/2019/12/Libertys-briefing-on-the-Bill-of-Rights-Bill-for-second-reading-HoC-July-2022_.pdf. See also Joint Civil Society briefing available at: https://www.libertyhumanrights.org.uk/wp-content/uploads/2019/12/Joint-Civil-Society-Briefing-on-the-Bill-of-Rights-Bill-for-Second-Reading-in-the-House-of-Commons-September-2022.pdf

[35] Human Rights Watch, *Automated hardship: How the Tech-Driven Overhaul of the UK's Social Security System Worsens Poverty,* 29 September 2020, available at: https://www.hrw.org/report/2020/09/29/automated-hardship/how-tech-driven-overhaul-uks-social-security-system-worsens

[36] Information Commissioner's Office, *ICO finds Metropolitan Police Service's Gangs Matrix breached data protection laws,* 16 November 2018, available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/11/ico-finds-metropolitan-police-service-s-gangs-matrix-breached-data-protection-laws/

[37] Liberty, *Legal challenge: Ed Bridges v South Wales Police,* available at: https://www.libertyhumanrights.org.uk/issue/legal-challenge-ed-bridges-v-south-wales-police/

[38] Foxglove, *Home Office says it will abandon its racist visa algorithm – after we sued them,* 4 August 2020, available at: https://www.foxglove.org.uk/2020/08/04/home-office-says-it-will-abandon-its-racist-visa-algorithm-after-we-sued-them/

[39] The App Drivers and Couriers Union, *Gig economy workers score historic digital rights victory against Uber and Ola Cabs*,

application of the law, our 'Big Data' society, and the increasing prevalence of ADM (especially during the coronavirus pandemic) these rights will only become more important – which makes the Government's attempts to erode them all the more staggering (though unsurprising when seen through the lens of the Government shifting to a pro-innovation, pro-technology approach).

QUESTION 6

What lessons, if any, can the UK learn from other countries on AI governance?

37. Numerous states and municipalities across the United States – from San Francisco, Oakland, and Boston – have banned ADM technologies like facial recognition outright including their acquirement, and the information derived from their use.[40] Companies at Silicon Valley – the birthplace of ADM – like Microsoft,[41] IBM,[42] and Amazon, have also ceased or put moratoria on the sales and production of ADM technologies, as well as taken steps to updating various internal AI standards and policies.

38. Closer to home, the European Parliament has adopted a non-binding resolution that police forces should be banned from using facial recognition and predictive policing algorithms.[43] The AI Act currently being scrutinised by the EU also recognises the level of harm caused by AI and categorises systems based on risk (with some systems deemed too risky to be used at all), and mandates a register of high-risk AI systems.[44] The UN High Commissioner for Human Rights, Michelle Bachelet, has also called for a "moratorium on the sale and use of artificial intelligence systems that pose a serious risk to human rights."[45]

39. In addition to various attempts to strengthen ADM governance, what these jurisdictions have in common are "algorithmic war stories" emerging as cautionary tales. In 2021, privacy watchdogs in Canada ordered facial recognition company Clearview AI to stop collecting, using and disclosing images of people without their

---

available at: https://www.adcu.org.uk/news-posts/gig-economy-workers-score-historic-digital-rights-victory-against-uber-and-ola-cabs

[40] Electronic Frontier Foundation, *The Movement to Ban Government Use of Face Recognition*, May 2022, available at: https://www.eff.org/deeplinks/2022/05/movement-ban-government-use-face-recognition

[41] https://www.theguardian.com/technology/2022/jun/22/microsoft-limits-access-to-facial-recognition-tool-in-ai-ethics-overhaul

[42] https://www.vox.com/recode/2020/6/10/21285658/ibm-facial-recognition-technology-bias-business

[43] Privacy International, *The EU Parliament took a stance against AI mass surveillance,* 7 Oct 2021. Available at: https://privacyinternational.org/news-analysis/4637/eu-parliament-took-stance-against-ai-mass-surveillance-what-are-global#:~:text=The%20European%20Parliament%20has%20adopted,ones%20used%20by%20Clearview%20AI.

[44] EU AI Act. Available at: https://artificialintelligenceact.eu/

[45] United Nations, *Urgent action needed over artificial intelligence risks to human rights*, 15 Sept 2021. Available at: https://news.un.org/en/story/2021/09/1099972

consent after its joint investigation found that the tech resulted in mass surveillance of Canadians and violated federal and provincial laws governing personal information.[46] Similarly in May 2022, following a joint investigation by the UK's Information Commissioner's Office and the Australian Information Commissioner (OAIC), Clearview AI was fined £7,552,800 for breaching UK data protection laws, after it used images of people that were collected from the web and social media to create a global online database that could be used for facial recognition. The ICO also issued an enforcement notice, ordering the company to "stop obtaining and using the personal data of UK residents that is publicly available on the internet, and to delete the data of UK residents from its systems."[47]

40. Best-selling books like Virginia Eubanks' *Automating Inequality* and Cathy O'Neil's *Weapons of Math Destruction* have charted a rise of a "new regime of data analytics" in the US that is restricting essential services – and in the process entrenching inequality and discrimination, expanding the surveillance state, and undermining access to justice. **It is Liberty's view that the UK Government heed these warnings that make clear and powerful arguments against the use of ADM.**

(December 2022)

[46] Jim Bronskill, *Provinces order Clearview AI to stop using facial recognition without consent*, The Canadian Press, 14 Dec 2021. Available at: https://globalnews.ca/news/8451440/clearview-ai-facial-recognition-order-stop/

[47] Information Commissioner's Office, *ICO fines facial recognition database company Clearview AI Inc more than £7.5m and orders UK data to be deleted,* 23 May 2022. Available at: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/05/ico-fines-facial-recognition-database-company-clearview-ai-inc/