Public Law Project

Public Law Project evidence submission on the Data Protection and Digital Information Bill (No. 2)

May 2023

Contents page

Summary and recommendations

1. The changes envisaged by the Bill will have serious implications for data subjects' rights, notably under articles 8 and 14 ECHR.

2. By lowering the threshold at which a subject access request may be refused, the Bill creates a risk of systemic breaches of data subjects' article 8 rights.

3. The Bill reverses the presumption that solely automated decisions cannot be made about a person where that decision has legal or similarly significant effects and allows for solely automated decisions in all contexts except where special category data is used. These changes could lead to serious and discriminatory effects on people's lives, including disproportionate impacts on marginalised groups, which has implications under article 14 ECHR.

4. The Bill requires significantly less information to be provided when undertaking Data Protection Impact Assessments, which will make establishing discrimination more difficult.

5. Recommendations

    - PLP recommends that the threshold for the refusal of data subjects' requests to exercise their rights of access, rectification and erasure by controllers is not changed; parliamentarians should therefore remove Clause 7 of the Bill. The existing protections in the GDPR for these rights need to be better enforced, rather than weakened.
    - PLP recommends that the current prohibition on solely automated decision-making under Article 22 is preserved, rather than narrowed.
    - The Secretary of State's power under the Bill to vary the safeguards in Clause 11 should be replaced with a power only to add safeguards.
    - Legislation is needed to broaden the application of safeguards, so that they are required in circumstances in which ADM plays a significant role in decision-making, but there is human review (and therefore not solely ADM). This must include requirements for transparency about the use of ADM, how the system works, and the role it plays in decision-making.
    - The proposed changes to DPIAs under Clause 17 of the Bill should not be pursued; existing, more detailed requirements should be retained.

Question 1: The Bill would make changes to the rights of data subjects under the UK GDPR, including altering the threshold at which data controllers may refuse to comply with a request made by a data subject and expanding when personal data can be processed for a reason other than that for which it was originally collected. Would these changes have any implications for data subjects' right to respect for their private lives under Article 8 ECHR?

Summary

6. These changes will have significant implications for data subjects' rights as protected under article 8 ECHR. By lowering the threshold at which a subject access request may be refused, the Bill creates a risk of systemic breaches of data subjects' article 8 rights.

The new 'vexatious or excessive' test: problems and implications

7. Clause 7 of the Data Protection and Digital Information Bill introduces a new standard at which data controllers may refuse to act upon a data subject's request for access, erasure or rectification (among others) where the request is 'vexatious or excessive'. The vague criteria to be considered in deciding whether a request is vexatious or excessive include "the nature of the request", "the relationship between the data subject and the controller", "the resources available to the controller", and to what extent it overlaps with previous requests. Under clause 32, the circumstances in which the ICO may refuse to act on a request is undergoing the same change in standard.

8. How exactly the 'vexatious and excessive' standard and the individual factors under clause 7 will be interpreted is unclear. In the context of Freedom of Information Requests, it has been held that the 'vexatious' test includes a consideration of whether there is a reasonable foundation that the information is of value to the requester or the public.[1] However, this is a completely inappropriate standard – in contrast to FOIAs, access to one's own personal data is a fundamental right, exercise of which should not require justification. This is particularly worrying for the right of access, without which there can be no meaningful exercise of any other data rights.[2] For instance, the claimant in *Catt*

[1] Liberty, 'Response to the Department of Digital, Culture, Media and Sports Consultation Data: A New Direction' (November 2021), https://www.libertyhumanrights.org.uk/wp-content/uploads/2021/11/Libertys-response-to-the-Department-of-Digital-Culture-Media-and-Sports-consultation-into-Data-A-new-direction.pdf, para. 73.

[2] AWO, 'Data Protection and Digital Information Bill: Impact on Data Rights' (March 2023), https://www.awo.agency/files/Data-Bill-No-2-Impact-on-Data-Rights.pdf, para. 11; Liberty, 'Response to the Department of Digital, Culture, Media and Sports Consultation Data: A New Direction' (November 2021), https://www.libertyhumanrights.org.uk/wp-content/uploads/2021/11/Libertys-response-to-the-Department-of-Digital-Culture-Media-and-Sports-consultation-into-Data-A-new-direction.pdf, para. 64; J. Ausloos, R. Mahieu and M. Veale, 'Getting Data Subjects Rights Right: A Submission to the European Data Protection Board from International Data Rights Academics, to Inform Regulatory Guidance', Journal of Intellectual Property, Information Technology and E-Commerce Law 10 (2020), https://www.jipitec.eu/issues/jipitec-10-3-2019/5031 (accessed 17.05.2023), para. 17.

v UK[3] was only able to discover that data about his attendance of protests was being unlawfully retained by making a subject access request.[4]

9. Furthermore, the Court of Appeal has held that data subjects may have "collateral purposes" for their request, such as litigation, and that this will not relieve data controllers from their obligation to respond.[5] Subject access requests are therefore not only an important gateway to exercise one's data protection rights, but also to vindicate one's rights, more generally, through litigation.

10. Evidence heard by the JCHR in 2019 suggested that even with the GDPR in its current form, individuals' rights to erasure and rectification were not always being adequately enforced.[6] The new 'vexatious or excessive' test proposed under the Bill can only lead to a worsening of the situation. It is likely to lead to increased numbers of refusals of legitimate requests,[7] with greater freedom for data controllers to refuse these on vague grounds.[8] Furthermore, AWO analysis suggests that the new test in combination with other measures introduced by the bill could lead to data subjects having to wait at least 20 months to resolve even basic breaches of their data rights.[9]

Data protection under article 8 ECHR

11. It is well-established that the right to protection of personal data is a fundamental part of the right to privacy under article 8 ECHR. The rights in relation to personal data protected under article 8 include the rights of access, rectification, and erasure.[10] Even the mere storing of information amounts to an interference with the applicants' right to respect for private life under article 8.[11]

12. Where such an interference occurs, this must be (1) in accordance with the law, (2) pursuant to a legitimate aim and (3) necessary in a democratic society. [12] Point (3) is most likely to have implications for the changes proposed by clause 7 of the Bill. To be "necessary in a democratic society", the interference must answer a "pressing social need", be proportionate to the legitimate aim pursued, and the reasons to justify the interference must be "relevant and sufficient", subject to the margin of

---

[3] 69 EHHR 7.

[4] Liberty, 'Response to the Department of Digital, Culture, Media and Sports Consultation Data: A New Direction' (November 2021), https://www.libertyhumanrights.org.uk/wp-content/uploads/2021/11/Libertys-response-to-the-Department-of-Digital-Culture-Media-and-Sports-consultation-into-Data-A-new-direction.pdf, para. 66.

[5] Norton Rose Fulbright, 'UK Court of Appeal allows data subject access requests to be made in furtherance of litigation' (July 2017), https://www.nortonrosefulbright.com/en-gb/knowledge/publications/8f893b33/uk-court-of-appeal-allows-data-subject-access-requests-to-be-made-in-furtherance-of-litigation; see *Dawson-Damer v. Taylor Wessing LLP* [2017] EWCA Civ 74 and I*ttihadieh v Cheyne Gardens & Ors and Deer v University of Oxford* [2017] EWCA Civ 121.

[6] Joint Committee on Human Rights, 'The Right to Privacy (Article 8) and the Digital Revolution' Third Report of Session 2019, *HC 122, HL Paper 14,* https://publications.parliament.uk/pa/jt201919/jtselect/jtrights/122/122.pdf, para 78.

[7] Liberty, 'Response to the Department of Digital, Culture, Media and Sports Consultation Data: A New Direction' (November 2021), https://www.libertyhumanrights.org.uk/wp-content/uploads/2021/11/Libertys-response-to-the-Department-of-Digital-Culture-Media-and-Sports-consultation-into-Data-A-new-direction.pdf, para. 71.

[8] AWO, 'Data Protection and Digital Information Bill: Impact on Data Rights' (March 2023), https://www.awo.agency/files/Data-Bill-No-2-Impact-on-Data-Rights.pdf, para. 11.

[9] AWO, 'Data Protection and Digital Information Bill: Impact on Data Rights' (March 2023), https://www.awo.agency/files/Data-Bill-No-2-Impact-on-Data-Rights.pdf, para. 18.

[10] 'Guide to the Case-Law of the European Court of Human Rights: Data Protection' (updated 31 August 2022), https://www.echr.coe.int/Documents/Guide_Data_protection_ENG.pdf, paras 3; 266; 277; 284.

[11] *Catt v. the United Kingdom*, application no. 43514/15 (2019), https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-189424%22]}, para. 93.

[12] *S. and Marper v. the United Kingdom,* application nos. 30562/04 and 30566/04 (2008), https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-90051%22]}, paras. 101-2; *Catt v. the United Kingdom,* application no. 43514/15 (2019), https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-189424%22]}, para. 109.

appreciation enjoyed by the State.[13]

13. The caselaw of the European Court of Human Rights ("ECtHR") has established that where personal data is collected and stored by public bodies, in particular where this is sensitive data going to a person's identity, there is a positive obligation to provide the individual with an "effective and accessible" procedure to allow them to have access to "all relevant and appropriate information".[14]

14. The ECtHR has held that there is a requirement for the decision-making process to be fair and to afford due respect to the interests safeguarded by it. This may require the existence of an effective procedural framework, which does not create an "insurmountable barrier" in the way of exercising these rights.[15] This includes a requirement to have applications processed within a reasonable time.[16] Safeguards in relation to these rights must be "practical and effective", not "theoretical and illusory".[17]

15. In *Catt v United Kingdom*, the ECtHR held that the safeguard provided by a data subject's right to access and erasure are only of limited impact where the controller refuses to delete the data and fails to provide an explanation for its continued retention. The Court further noted that it would be entirely contrary to the need to protect an individual's article 8 rights if a public body could create a database that was difficult to review or edit, and then use this as a justification to refuse to remove information from that database.[18]

16. The new 'vexatious or excessive' test creates a potential risk of systemic breaches under article 8. Controllers will have a wider discretion to refuse requests, including based on an assessment of their own resources, and whether the request is "intended to cause distress". Will a controller therefore be able to make vague arguments about a lack of resources and overly complicated requests, which it may argue are intended to cause distress? It would be unlikely that such a justification for interfering with a data subject's rights would stand up to the requirements for meeting a "pressing social need", or indeed for the reasons for interference being "relevant and sufficient".

17. This may further run contrary to a number of the specific requirements established by ECtHR caselaw set out above, including for "effective and accessible" procedures for accessing one's data, for "practical and effective" safeguards, and to give proper reasons when a request is refused. Furthermore, given legal consultancy AWO's analysis of potential delays caused by these new rules,[19] there is a chance that systemic breaches of the requirement for reasonable timeframes will arise.

---

[13] *Ibid.*

[14] 'Guide to the Case-Law of the European Court of Human Rights: Data Protection' (updated 31 August 2022), https://www.echr.coe.int/Documents/Guide_Data_protection_ENG.pdf, para. 121; see, for instance, *Haralambie v. Romania,* application no. 21737/03 (2009).

[15] 'Guide to the Case-Law of the European Court of Human Rights: Data Protection' (updated 31 August 2022), https://www.echr.coe.int/Documents/Guide_Data_protection_ENG.pdf, para. 297.

[16] 'Guide to the Case-Law of the European Court of Human Rights: Data Protection' (updated 31 August 2022), https://www.echr.coe.int/Documents/Guide_Data_protection_ENG.pdf, para. 303.

[17] 'Guide to the Case-Law of the European Court of Human Rights: Data Protection' (updated 31 August 2022), https://www.echr.coe.int/Documents/Guide_Data_protection_ENG.pdf, para. 294; see, for instance, *M. K. v. France*, application no. 19522/09 (2013) paras. 44-47.

[18] *Catt v. the United Kingdom*, application no. 43514/15 (2019), https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-189424%22]}, para. 122; 127.

[19] AWO, 'Data Protection and Digital Information Bill: Impact on Data Rights' (March 2023), https://www.awo.agency/files/Data-Bill-No-2-Impact-on-Data-Rights.pdf, para. 11.

Case study

The Gangs Violence Matrix

18. The Gangs Violence Matrix ('GVM') is an intelligence tool used by the Metropolitan Police to "risk-assess" gang members in London. Its stated aim is to reduce gang-related violence.[20] In 2018 the ICO concluded that the Metropolitan Police Service's use of the matrix had led to serious breaches of data protection laws. Their investigation found that data sharing with third parties and the failure to distinguish between high and low risk individuals created a potential for disproportionate action against the predominantly young Black men on the database.[21] This included individuals being recorded on the Matrix simply because they were victims of gang-related crimes.[22] The only way for individuals to find out whether their data is on the database, and to exercise their rights of erasure and rectification, is to make a subject access request.[23]

19. The way in which the GVM has operated therefore has serious human rights implications, notably under articles 8 and 14 ECHR. Under article 8, safeguards for data subjects are particularly important where their data is automatically processed for police purposes, especially where they have not been convicted of a crime.[24] The Met Police has recently settled a case with Liberty, in which it admitted the operation of the GVM had breached data subjects' article 8 rights. It agreed to change the operation of the database, including introducing a mechanism allowing individuals to apply for information on whether they are on the GVM.[25]

20. Had these provisions of the Data Bill been in force, it would have given the Met Police additional scope to deny requests from individuals – who were wrongly on the GVM – to be informed on whether they are on the GVM and/or to be removed. This would have likely led to even more widespread and serious article 8 violations. For example, might the Met Police have been able to argue that a request for access or erasure is an 'abuse of process' (clause 7(3)(5)(c) of the Bill) if they wrongly believe someone to be an active gang member? The new standard under clause 7 may lead to vague refusals of genuine requests for access or erasure which will significantly dilute the procedural safeguards that exist in relation to databases such as the GVM.

---

[20] https://www.met.police.uk/police-forces/metropolitan-police/areas/about-us/about-the-met/gangs-violence-matrix/.
[21] Liberty, 'Response to the Department of Digital, Culture, Media and Sports Consultation Data: A New Direction' (November 2021), https://www.libertyhumanrights.org.uk/wp-content/uploads/2021/11/Libertys-response-to-the-Department-of-Digital-Culture-Media-and-Sports-consultation-into-Data-A-new-direction.pdf, para. 67.
[22] Information Commissioner, 'Enforcement Notice to the Commissioner of Police of the Metropolis' (13 November 2018), https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/about-us/gangs-violence-matrix/ico-enforcement-notice.pdf, para. 16.
[23] Liberty, 'Response to the Department of Digital, Culture, Media and Sports Consultation Data: A New Direction' (November 2021), https://www.libertyhumanrights.org.uk/wp-content/uploads/2021/11/Libertys-response-to-the-Department-of-Digital-Culture-Media-and-Sports-consultation-into-Data-A-new-direction.pdf, para. 67.
[24] *S. and Marper v. the United Kingdom,* application nos. 30562/04 and 30566/04 (2008), https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-90051%22]}, paras. 103; 122; 124.
[25] Liberty, 'Met to overhaul 'racist' Gangs Matrix after landmark legal challenge' (11 November 2022), https://www.libertyhumanrights.org.uk/issue/met-to-overhaul-racist-gangs-matrix-after-landmark-legal-challenge/.

21. The Bill may also have implications for how the Met Police's new system will function. If the Met Police seeks to rely on the new standards introduced by the Bill, this may dilute the improvements it will make to the system following the settlement of the legal case against Liberty.

Recommendations

22. PLP recommends that the threshold for the refusal of data subjects' requests by controllers is not changed; parliamentarians should therefore remove Clause 7 of the Bill. The existing protections in the GDPR for these rights need to be better enforced, rather than weakened.

Question 3: What are the likely human rights implications of the new approach to automated decision-making under clause 11 of the Bill, and would the proposed measures be compatible with human rights law, including Article 14 ECHR on the prohibition of discrimination in the enjoyment of other Convention rights? Are there sufficient safeguards and rights of challenge in relation to automated decision-making?

Summary

23. The Bill reverses the presumption that solely automated decisions cannot be made about a person where that decision has legal or similarly significant effects. These changes could lead to serious and discriminatory effects on people's lives, including disproportionate impacts on marginalised groups, which has implications under article 14 ECHR.

The new approach under the Bill

24. Presently under Article 22 of the GDPR as incorporated into UK law there is a prohibition on solely automated decision-making. A solely automated decision, one that does not contain meaningful human review, cannot be made about a person where that decision has legal or similarly significant effects except where that person expressly consents to it, it is necessary for the performance of a contract, or it is provided for in law.

25. The Bill as drafted proposes to essentially reverse that presumption and allow for solely automated decisions in all contexts except where special category data is used. Special category data is a much narrower category of data which includes health and sexual orientation data. PLP is concerned by this change because automated decisions can have serious and discriminatory effects on people's lives

without using special category data. Examples include decisions concerning access to financial products, educational decisions like the UK's A-level algorithm scandal, or the SyRI case in the Netherlands where innocuous datasets such as household water usage were used to accuse individuals of benefit fraud.[26] Australia's 'Robodebt Scandal' involved a solely automated data matching service which incorrectly sought repayment of benefits from over 300,000 people because the system was operating without human oversight. The scandal had an enormous human cost, and the Australian Government is currently paying millions in compensation to those affected.[27]

Article 14 of the Human Rights Act

26. Automated systems pose a heightened risk of discrimination. The Public Law Project considers that the removal of the prohibition on solely automated decisions will greatly increase the number of people subject to decisions by automated systems without human oversight and therefore increase the risk that people will be discriminated against by these systems. This is especially concerning when it is marginalised groups who are often subject to increased scrutiny and decision-making by algorithmic technology. Furthermore, the lack of transparency surrounding these systems makes proving discrimination difficult for claimants.

27. Article 14 of the Human Rights Act 1998 provides: "The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status."[1] Examples of 'other status' that have emerged in the case law are sexual orientation, illegitimacy, marital status, trade union membership, transsexual status, imprisonment, age and disability.[28]

Automated systems and discrimination

28. Bias can be 'baked in' to ADM systems for a variety of reasons, including as a result of problems in the design of the system or its training data. If the training data is unrepresentative, then the algorithm may systematically produce worse outcomes when applied to a particular group. A high-profile example of this was the South Wales Police's (SWP) use of facial recognition technology. Before the High Court, there was evidence that, due to the imbalance in the representation of different groups in the training data, automated facial recognition was less accurate at recognising the faces of people of colour and women.[29]

29. A Council of Europe study has noted that concerns around Article 14 are prevalent when it comes to ADM.[30] Big data algorithms may use features or criteria of the individual which serve as proxies for

---

[26] C van Veen, 'Profiling the Poor in the Dutch Welfare State. Report on Court Hearing in Litigation in the Netherlands about Digital Welfare Fraud Detection System "SyRI"' (Center for Human Rights and Global Justice, 1 November 2019), https://chrgj.org/2019/11/01/profiling-the-poor-in-the-dutch-welfare-state/ accessed 25 April 2023, as discussed in M Busuioc, D Curtin and M Almada 'Reclaiming transparency: Contesting the logics of secrecy within the AI Act' (2022) European Law Open, 1-27.

[27] Karen Yeung 'The New Public Analytics as an Emerging Paradigm in Public Sector Administration' (2022) 27(2) Tilburg Law Review 1, 2.

[28] Equality & Human Rights Commission, 'Article 14: Protection from Discrimination' (updated 03.06.2021), https://www.equalityhumanrights.com/en/human-rights-act/article-14-protection-discrimination#:~:text=The%20Human%20Rights%20Act%20makes,%2C%20birth%20or%20other%20status'.

[29] *R (Bridges) v Chief Constable of South Wales Police and others* [2020] EWCA Civ 1058.

[30] Committee of Experts on Internet Intermediaries (Council of Europe), *Study on the Human Rights Dimensions of Automated Data Processing Techniques (in Particular Algorithms) and Possible Regulatory Implications* (2018), https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5, pp. 26-8.

protected characteristics such as race, gender or age. An algorithm may choose to discriminate against a group of users by using a feature which is not itself protected, but which correlates to a high degree with a protected characteristic. An example of this is the use of postcodes by automated systems which in segregated areas can operate as proxies for race.[31]

30. Similarly, the House of Commons Science and Technology Select Committee noted in 2018 that ML algorithms can perpetrate discrimination through learning discriminatory relationships between data.[32] The UN Special Rapporteur on the rights of persons with disabilities has called on States and institutions to acknowledge the negative impacts of AI on persons with disabilities, which arise from poor or unrepresentative data sets, a lack of transparency, a short-circuiting of the obligation of reasonable accommodation, and a lack of effective remedies.[33] The Greater Manchester Coalition for Disabled People has collected anecdotal evidence that a high percentage of their group has been flagged for investigation by the DWP's automated systems.[34] Yet, when asked by Debbie Abrahams MP at a Work and Pensions Committee meeting on 24 November 2021 on the subject of the 2021-22 Accounts, the DWP was unable to say what proportion of the people being investigated for benefit fraud are disabled.[35]

Impacts on marginalised groups

31. Many of the ADM systems PLP is aware of appear to have an unequal impact on marginalised groups and/or groups with protected characteristics. The Equality Impact Assessment disclosed for the Home Office's sham marriage triage tool included a graph showing that Indian couples were flagged for investigation for entering into a potential sham marriage around 10% of the time and Pakistani nationals around 15% of the time. Bulgarian and Greek couples were flagged for investigation at a rate of between 20% and 25% despite making up a much lower proportion of the proposed marriages between a UK and non-UK national than couples from Pakistan and India.[36] The First Tier Tribunal in *Public Law Project v Information Commissioner* accepted that the tool exhibited prima facie indirect discrimination.[37]

32. It appears that the DWP's automated tool(s) for detecting possible fraud and error in Universal Credit claims may have a disproportionate impact on people of certain nationalities. The Work Rights Centre have told the Public Law Project that, since August 2021, they have been contacted by 39 service users who reported having their Universal Credit payments suspended. Even though the charity advises a range of migrant communities, around 35 of the service users who reported having their payments suspended were Bulgarian.[38]

---

[31] Marion Oswald and others 'Algorithmic risk assessment policing models: lessons from the Durham HART model and 'Experimental' proportionality' (2018) Information & Communications Technology Law, 27:2, 223-250.

[32] Allen, 'Artificial Intelligence, Machine Learning, Algorithms and Discrimination Law: The New Frontier', *Michael Rubenstein Conference: Discrimination Law in 2020* (2020), https://global-uploads.webflow.com/5f57d40eb1c2ef22d8a8ca7e/606710cc05a1b6228ae758fc_Discrimination-Law-in-2020.FINAL_-1.pdf, para. 76.

[33] R. Allen and D. Masters, 'A Difficult Different Discrimination: Artificial Intelligence and Disability', *ai Law* (17 March 2022), https://ai-lawhub.com/2022/03/17/a-difficult-different-discrimination-artificial-intelligence-and-disability/.

[34] https://www.foxglove.org.uk/2021/12/01/secret-dwp-algorithm/.

[35] https://parliamentlive.tv/event/index/d4766433-5e00-4060-8e24-a5e4030da3d3?in=10:47:54.

[36] *Public Law Project v Information Commissioner* [2023] UKFTT 0228 (GRC) [45].

[37] *Public Law Project v Information Commissioner* [2023] UKFTT 0228 (GRC) [62].

[38] https://publiclawproject.org.uk/content/uploads/2023/01/PLP-submission-Science-and-Technology-Committee-Call-for-evidenceas-submitted.pdf

Lack of transparency

33. The Bill contains an important safeguard against opacity. It provides that when a data subject is subject to a solely automated decision they must be notified of that fact and provided with information about the decision.

34. However, the Bill also allows for the Secretary of State to vary the safeguards provided for under the Bill. The Public Law Project is concerned about this. Given the prohibition on solely automated decision-making is being removed, it is important that stringent safeguards are maintained; including the right to be informed of an automated decision, the right to receive meaningful information about the decision and the right to request human review of the decision.

35. One of the biggest challenges with automated decision-making in the UK at present is the opacity around automated decisions. When people are subject to a decision that is partly or solely automated, they are not always informed of this. Individuals are unable to challenge an automated decision when they do not know it was automated in the first place. Individuals who are investigated by the Home Office for entering into a potential sham marriage are not informed that they have been selected for investigation by an automated triage tool. The MP for Edmonton, Kate Osamor, noted in Parliament that 29 Bulgarian nationals in her constituency had their universal credit payments suspended on the basis of a fraud investigation, and one constituent received no benefits for 11 months.[39] None of those individuals were told that it was an automated model used by the DWP which had flagged their case for review, or of the criteria used by the model.

36. Opacity also makes it difficult to establish discrimination. An applicant cannot make the case that the criteria used by the system are directly or indirectly discriminatory when it is not known which criteria have been used in reaching the output.

37. Therefore, it is vital that the safeguards against opacity in the Bill are maintained as they provide for an individual to be notified when they are subject to a solely automated decision and to receive information about the nature of the decision.

38. The Bill as drafted allows for the Secretary of State to vary any safeguards by statutory instrument, meaning that any changes will receive little, if any, parliamentary oversight. This is inappropriate: only the power to add additional safeguards should be retained in the Bill, not the power to vary.

Data Protection Impact Assessments

39. PLP is also concerned about the proposed changes to Data Protection Impact Assessments ('DPIAs'). Currently, a DPIA must be carried out for all high-risk processing activities, and it must include:

    (a) a general description of the envisaged processing operations;
    (b) an assessment of the risks to the rights and freedoms of data subjects;
    (c) the measures envisaged to address those risks;
    (d) safeguards, security measures and mechanisms to ensure the protection of personal data… taking into account the rights and legitimate interests of the data subjects and other persons concerned."

40. DPIAs are only required for high-risk processing activities and as a result they do not place an undue burden on data processors. The ICO calls DPIAs an 'essential part' of a data processors' 'accountability

[39] HC Deb 26 January 2002, vol 707, col 392WH.

obligations'.[40] DPIAs help with the identification and minimisation of risks before they arise, and they provide information to the data subject with which they can subsequently assess the lawfulness of the processing activity. The DPIA provided key information about Automated Facial Recognition technology in the case of *Bridges v South Wales Police*.[41] The Home Office also undertook to provide disclosure of the DPIA for any new visa streaming tool it developed as part of its settlement with the Joint Council for the Welfare of Immigrants who challenged the Home Office's visa streaming tool which directly discriminated on the basis of nationality.[42]

41. The Bill's changes to DPIAs require significantly less information to be provided. Under clause 17 they will not have to provide much more additional information than is currently required for privacy notices, a standard requirement on data controllers for all processing activities. This seems anachronistic given that DPIAs are reserved for high risk processing activities.

42. Under the Bill DPIAs have to contain:

    (a) a summary of the purposes of the processing,
    (b) an assessment of whether the processing is necessary for those purposes,
    (c) an assessment of the risks to the rights and freedoms of individuals referred to in subsection (1), and
    (d) description of how the controller proposes to mitigate those risks.

43. This means data processors will no longer be required to give details as to the processing operations and how data is being used. DPIAs currently require data processors to explain how they are doing the processing, which can include which data sources they are using, how that data has been trained and how the automated tool interacts with any human decision-maker. The new DPIA proposals under the Bill only require details on the purpose for processing, not how the processing is being done. This will make establishing discrimination more difficult as data subjects will have less information with which to assess the lawfulness of the operation of the system.

Case studies

The Home Office's 'Visa Streaming Tool'

44. Automated systems can both directly and indirectly discriminate. In the case of the Home Office's 'Visa Streaming Tool' the Home Office used a system which automated the risk profiling of entry clearance visa applications to the UK. The tool allocated all applicants for entry clearance to the UK to one of three streams: red, amber or green. If an applicant was from a list of certain nationalities they would automatically be sorted into the red category. The tool then matched all other applicants with risk profiles constructed by the Home Office and the tool sorted all applicants into red, amber and green categories based on their individual risk profiles. Again, these risk profiles used nationality as one of the criteria for determining an applicant's level of risk of over-staying. Whether an individual was allocated into the red, amber or green category determined the level of scrutiny that Home

[40] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/what-is-a-dpia/
[41] *R (Bridges) v Chief Constable of South Wales Police and others* [2020] EWCA Civ 1058.
[42] https://www.jcwi.org.uk/news/we-won-home-office-to-stop-using-racist-visa-algorithm.

Official officials would give to the visa entry applications and the time be spent on each application. Officers had benchmarks for example at the Sheffield Decision Centre their targets were to examine 55 'green' applications or 18 'red' applications a day.[43]

45. There is evidence in the Home Office's own guidance documents that even though the tool was supposed to only sort the applications, officials treated the tool as providing a default assessment of the risk posed by an application. Data shows that 'red' applications were refused at a much higher rate than 'green' applications. For example, at the Croydon decision-making centre in 2019, 45 per cent of red applications were refused and 0.5 per cent of green applications.[44]

46. Following the initiation of a legal challenge by the civil society organisation Joint Council for the Welfare of Immigrants (JCWI) and Foxglove alleging that the visa streaming tool was directly discriminatory on the basis of nationality, the Home Office suspended its use in August 2020.[45]

Durham Constabulary's Harm Assessment Risk Tool

47. Durham Constabulary's Harm Assessment Risk Tool ('HART') was used by custody officers to decide if someone convicted of a crime should be referred to a rehabilitation program called 'Checkpoint'. If HART deems an applicant high risk they would not be referred to the program, only those deemed a moderate risk of reoffending were eligible. HART used a machine learning tool known as "random forest technique". The tool used 34 predictors, 29 relate to prior offending. Oswald explains that random forest models work by modelling an 'extremely large number of separate nodes'.[46]

48. The 29 features relating to prior offending were combined with personal characteristics such as age and gender, as well as postcode. The primary postcode predictor was limited to the first four characters of the postcode, and usually encompassed a large geographic area. A data point such as this can still risk a kind of feedback loop that can perpetuate or amplify existing patterns of offending.[47] If the police respond to forecasts by targeting their efforts on the highest-risk postcode areas, then more people from these areas will come to police attention and be arrested than those living in lower-risk, untargeted neighbourhoods.[48] These arrests become outcomes that are used to generate later iterations of the same model, leading to an 'ever-deepening cycle of increased police attention'.[49]

[43] Joe Tomlinson and Jack Maxwell, *Experiments in Automating Immigration Systems* (Bristol University Press 2021).
[44] Joe Tomlinson and Jack Maxwell, *Experiments in Automating Immigration Systems* (Bristol University Press 2021).
[45] https://www.jcwi.org.uk/news/we-won-home-office-to-stop-using-racist-visa-algorithm.
[46] Marion Oswald, 'Algorithm-assisted decision-making in the public sector: framing the issues using administrative law rules governing discretionary power' (2018) 376 Philosophical Transactions of the Royal Society.
[47] https://digi-con.org/ai-transparency-tag-register/.
[48] https://digi-con.org/ai-transparency-tag-register/.
[49] Marion Oswald and others 'Algorithmic risk assessment policing models: lessons from the Durham HART model and 'Experimental' proportionality' (2018) Information & Communications Technology Law, 27:2, 223-250.

Recommendations

49. PLP recommends that the current prohibition on solely automated decision-making under Article 22 is preserved, rather than narrowed.

50. The Secretary of State's power under the Bill to vary the safeguards in Clause 11 should be replaced with a power only to add safeguards.

51. Legislation is needed to broaden the application of safeguards, so that they are required in circumstances in which ADM plays a significant role in decision-making, but there is human review (and therefore not *solely* ADM). This must include requirements for transparency about the use of ADM, how the system works, and the role it plays in decision-making.

52. The proposed changes to DPIAs under Clause 17 of the Bill should not be pursued; existing, more detailed requirements should be retained.

Contact

Luke Robins-Grace
Communications Director
l.robins-grace@publiclawproject.org.uk

Alexandra Sinclair
Research Fellow
a.sinclair@publiclawproject.org.uk

Rachel Solomon
Research Assistant
r.solomon@publiclawproject.org.uk

Public Law Project is an independent national legal charity.

We are researchers, lawyers, trainers, and public law policy experts.

For over 30 years we have represented and supported individuals and communities who are marginalised through poverty, discrimination, or disadvantage when they have been affected by unlawful state decision-making.

Our vision is a world where the state acts fairly and lawfully. Our mission is to improve public decision making, empower people to understand and apply the law, and increase access to justice.

We deliver our mission through casework, research, policy advocacy, communications, and training, working collaboratively with colleagues across legal and civil society.

Public Law Project contributes and responds to consultations, policy proposals, and legislation to ensure public law remedies, access to justice, and the rule of law are not undermined.

We provide evidence to inquiries, reviews, statutory bodies, and parliamentary committees and we publish research and guides to increase understanding of public law.

Public Law Project's research and publications are available at:

www.publiclawproject.org.uk/resources-search/