Briefing on Clause 14

Data Protection and Digital Information Bill (No. 2)

House of Lords

Committee Stage

March 2024

For further information contact

Ellen Lefley, Lawyer, elefley@justice.org.uk

JUSTICE, 2nd Floor Lincoln House, 296-302 High Holborn, London, WC1V 7JH

email: admin@justice.org.uk website: www.justice.org.uk

Introduction

1. JUSTICE is a cross-party law reform and human rights organisation working to strengthen the justice system. It is the UK section of the International Commission of Jurists. Our vision is of fair, accessible and efficient legal processes in which the individual's rights are protected and which reflect the country's international reputation for upholding and promoting the rule of law.

2. This briefing addresses Clause 14 of the Data Protection and Digital Information Bill ("**DPDI Bill**") which amends the current right not to be subject to solely automated decision making, including profiling.

3. **In summary, JUSTICE opposes Clause 14, and encourages Peers to support Lord Clement Jones in his intention to oppose that Clause 14 stand part of the Bill.**

4. This briefing is sent in tandem with a separate joint briefing, from JUSTICE and the Public Law Project ("**PLP**"). In summary, the joint briefing sets out JUSTICE's and PLP's support for new clause amendments 74-78 after Clause 14, tabled by Lord Clement-Jones, and encourages Peers to support those amendments. They are:

    a) A statutory duty on public sector actors to have 'due regard' to ensuring automated decision systems are responsible and minimise harm to individuals and society at large, (**amendment 76**); and

    b) A statutory transparency requirement, placing the requirement for public sector actors to comply with the ATRS on a statutory footing (**amendments 74, 75, 77 and 78).**

Clause 14

5. Currently, individuals have a right not to be subject to significant decisions based solely on automated processing of their personal data without any meaningful human involvement,[1] with certain specified exceptions.[2]

6. Clause 14 of the Bill restricts this right to only those decisions involving "special category data". This is personal data revealing racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; biometric data (used for

[1] Article 22 UK GDPR and ss. 49-50 Data Protection Act 2018

[2] Exceptions are explicit consent; necessity for performance of a contract; or when authorised by a law which suitably protects the data subject's rights, freedoms and legitimate interests – Article 22, UK GDPR

identification purposes); data concerning health; data concerning a person's sex life; and data concerning a person's sexual orientation.

7. For decisions using personal data which is not special category data, the right is removed. Instead, Clause 14 creates a new starting point that entirely automated decision making ("**ADM**") including profiling, is allowed.

Problems with Clause 14

8. This new regime provides inadequate protections for individuals from unfair and discriminatory decisions for two reasons:

   a) Problem 1: the limited right that remains – not to be subject to ADM using special category data – is too narrow to achieve non-discriminatory outcomes; and

   b) Problem 2: the safeguards for the ADM which is being broadly permitted, using personal but not special category data, are insufficient.

Problem 1: The limited right that remains is too narrow to achieve non-discriminatory outcomes

9. Firstly, the Bill preserves the right not to be subject to ADM for special category data only. This acknowledges that automated systems are trained on imperfect data, and can contain 'legacies of discrimination',[3] which embed and reproduce existing social biases.

10. For example, facial recognition software uses biometric data for identification (which is special category data). There have been various examples of facial recognition software which have produced discriminatory outputs, the literature particularly highlighting the potential for more inaccurate results for women and those with darker skin.[4]

11. However, it is not true to suggest – as the Bill does – that to allow all ADM *except for* that using special category data is therefore safe**.** In fact, **significant discrimination can occur when there is no special category data, because**:

[3] House of Lords Justice and Home Affairs Committee, "Technology rules? The advent of new technologies in the justice system" 1st Report of Session 2021 – 22, §158 at p.58.

[4] For a comprehensive explanation of bias in facial recognition technologies, see David Leslie, *Understanding bias in facial recognition technologies: an explainer* (The Alan Turing Institute, 2020).

a) **non-special categories of data can become proxies for special category data**. For example, addresses indicating someone lives in a community which has a high population of individuals from a particular ethnic origin.

b) **Furthermore, special category data does not capture all possible data which could lead to discrimination**. For example, data of someone's sex or gender is not included in special category data, despite sex and gender reassignment both being protected characteristics under the Equality Act 2010.[5]

12. Indeed, there are numerous examples of ADM in such contexts which have produced discriminatory effects:

a) The COMPAS tool used in the US to assist with criminal sentencing gives a score of "risk" of reoffending based on several data points about the individual, including characteristics and personal history. It does not collect or process race or ethnic origin as an explicit data point. However, an investigation by non-profit news organisation, Propublica, still found embedded racial discrimination in the tool: Black defendants were more likely than White defendants to receive a "false positive" from the tool, i.e. be incorrectly judged to be at a higher risk of recidivism, while White defendants were more likely than Black defendants to receive a false negative, i.e. be incorrectly flagged as low risk.[6]

b) In 2018, Amazon used a machine learning artificial intelligence tool to make recruitment decisions. The tool was supposed to be gender neutral and did not collect or process the sex of the applicant as a discrete data point. However despite this, it began discriminating on the basis of sex, perpetuating an existing disparity in the workforce, which was majority male.[7]

c) The infamous Dutch case of SyRI, which involved ADM in determining benefits allocation, processed data in non-sensitive categories including but not limited to name, address, date of birth, gender, tax, work, history of administrative measures and sanctions being applied against them, education, pension, housing, and health

[5] There are some circumstances that sex or gender could be included in health data and/or data of their sexual orientation, but it is not always the case that it will be so.

[6] See Julia Angwin, Jeff Larson, Surya Mattu and Lauren Kirchner, 'Machine Bias' and 'How we analysed the COMPAS recidivism algorithm', *Propublica* (23 May 2016).

[7] See original Reuters report as archived by the Irish Times: Jeffrey Dastin. "Amazon scraps secret AI recruiting tool that showed bias against women". (2018)

care insurance.[8] SyRI was found to violate individuals rights under Article 8 paragraph 2 ECHR[9] the Dutch Court stating that:

"*the right to respect for private life in the context of data processing concerns the right to equal treatment in equal cases, and* ***the right to protection against discrimination, stereotyping and stigmatisation***." (Emphasis added).[10]

13. The ECHR Impact Assessment of the Bill, which was updated in December 2023, recognises this potential for discriminatory effect in contravention of human rights law:

It is acknowledged that AI systems are capable of reproducing and augmenting the patterns of discriminatory treatment that exist in society. [...] [T]here is a risk that the increase in scope of Article 22 processing could potentially lead to discrimination under Article 14 [read with Article 8".[11]

14. Similarly, in the Public Sector Equality Duty assessment, it was noted that,

"*The proposals around reforming Article 22 could potentially lead to an increase in automated decision-making including profiling which would result in an increase in the number of legal or similarly significant decisions made about individuals. […]* ***The government acknowledges that historically automated decision making has had a disproportionately detrimental effect upon people with protected characteristics, for example on the basis of race. If left without further mitigation, this could perpetuate inequalities by increasing the number of decisions made about people based on their protected characteristics***." (Emphasis added).[12]

15. JUSTICE does not consider that the proposed mitigations against groups with protected characteristics – namely, the AI White Paper (discussed below), awaited proposals to test AI-driven ADM, and legacy legal frameworks of Equality Act 2010 and the Human Rights

[8] See list of data categories which were qualified for processing in SyRI contained in §4.17 of the judgment in NJCM et al. v The Dutch State (2020) The Hague District Court ECLI: NL: RBDHA:2020:1878 (SyRI). English translation of the judgment is available at https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBDHA:2020:1878.

[9] Ibid at §6.7.

[10] Ibid at §6.24.

[11] Department for Science, Innovation & Technology and the Department for Work & Pensions, "Impact Assessment: Data Protection and Digital Information (No. 2) Bill: European Convention on Human Rights Memorandum" (updated 20 December 2023) at §§21 and 25.

[12] Department for Science, Innovation & Technology and Department for Work & Pensions, "Impact assessment: Public Sector Equality Duty assessment for Data Protection and Digital Information (No. 2) Bill" (updated 20 December 2023) at §64.

Act 1998 – address the issue of imperfect data inputs likely resulting in ADM reproducing systemic biases.

Problem 2: The safeguards for the ADM which is being permitted, using personal but not special category data, are inadequate.

16. Clause 14 creates a new starting point for all ADM using personal but not special category data: it is allowed, including profiling, provided certain safeguards are in place.

17. The safeguards are that controllers must provide information of the decision, and they must have measures in place which enable individuals to make representations, obtain human intervention, and contest decisions.

18. **These safeguards are inadequate, for 3 reasons**:

    a) **They shift the burden to the individual.** The permissive regime shifts the starting point to allow ADM and profiling. The safeguards simply require these routes of information and redress to be available to the individual: the onus is on the individual to complain if the ADM they have been subject to is unfair, discriminatory or even unsafe.

    b) **There is no obligation to provide any safeguards before the decision is made.** Neither the Bill nor its ancillary material indicate what the content of this 'information' is expected to be, nor the timescales in which that information is to be given. There is nothing to say when representations or contest may be heard, when human intervention may be sought or the level of that intervention. This not only offends the core principles of fair decision-making: the right to advance notice and representations.[13] It also means that there is no protections against harm being incurred before an individual knows about it.

    c) **The Secretary of State has delegated powers to vary the safeguards by regulations**. She can also state conclusively what does or does not satisfy them.[14] These are broad powers which could undermine further the sufficiency of the safeguards in practice.

[13] *The duty to give advance notice and an opportunity to be heard to a person against whom a draconian statutory power is to be exercised is one of the oldest principles of what would now be called public law*. *Bank Mellat v HM Treasury* [2013] UKSC 39 at §29

[14] Draft Article 22D in Clause 14

19. **There is therefore an entirely inadequate basis upon which Parliament can be satisfied that the Bill will safeguard individuals from harmful ADM before it is too late. In fact, the effect of the Bill will be to do the opposite: to permit unfair and unsafe ADM to occur, including discriminatory profiling ADM, which causes harm to individuals. It then places the burden on the individual to complain, without providing for any adequate safeguards which will guarantee their ability to do so before the harm is already incurred.**

Solutions to Clause 14

20. JUSTICE considers that the deployment of ADM under Clause 14 risks automating harm, including discrimination, without adequate safeguards.

21. **We therefore urge Peers to support Lord Clement-Jones in opposing that Clause 14 stand part of the Bill.**

22. **We also urge Peers to support** amendments 74-78 after Clause 14, tabled by Lord Clement-Jones, as discussed in our separate joint briefing, from JUSTICE and the Public Law Project ("**PLP**"), sent alongside this briefing. In summary, the joint briefing sets out JUSTICE's and PLP's support for:

    a) A statutory duty on public sector actors to have 'due regard' to ensuring automated decision systems are responsible and minimise harm to individuals and society at large, (**amendment 76**); and

    b) A statutory transparency requirement, placing the requirement for public sector actors to comply with the ATRS on a statutory footing (**amendments 74, 75, 77 and 78).**