Proving algorithmic discrimination in government decision-making

Jack Maxwell[[1]](#footnote-1)\* and Joe Tomlinson[[2]](#footnote-2)\*\*

Public Law Project, London, United Kingdom and University of York, United Kingdom

Public bodies in the United Kingdom are increasingly using algorithms and big data to make decisions. While there is growing awareness of the risks of algorithmic discrimination, it can be very difficult to establish that a specific algorithm is in fact discriminatory. This raises the question of how courts should allocate the burden of testing and proving whether a government algorithm is discriminatory, as between the government and the person affected. In *R (Bridges) v South Wales Police* [2020] EWCA Civ 1058, the England and Wales Court of Appeal found that public bodies must take positive steps to identify and address risks of algorithmic discrimination. This note explores the decision in *Bridges* and its implications for algorithmic decision-making in government. It suggests that *Bridges*, alongside recent decisions in Canada and the Netherlands, forms part of a broader trend: the courts are placing the burden of testing and reviewing potentially discriminatory algorithms on government, rather than the general public.

Keywords: algorithm; automated decision-making; discrimination; bias; facial recognition; judicial review

1. Introduction

Public bodies in the United Kingdom are increasingly using algorithms and big data to make decisions. The Home Office uses algorithms to process applications for the European Union Settlement Scheme.[[3]](#footnote-3) Police use algorithms to highlight crime hot spots, assess whether a particular person is likely to commit an offence, and identify people in public places.[[4]](#footnote-4) Local authorities use algorithms to predict whether a child is at risk of abuse or neglect, and to evaluate applications for housing benefit and council tax reduction.[[5]](#footnote-5)

As public sector algorithms become more prevalent, so too do risks of algorithmic discrimination.[[6]](#footnote-6) A range of different wrongs in data-driven decision-making can be brought under the banner of algorithmic discrimination, but two are particularly relevant.[[7]](#footnote-7) First, where algorithm is trained on data drawn mostly from a particular group of people, it may systematically produce worse outcomes when applied to different groups of people. Second, where an algorithm is trained on data which reflects existing inequalities between different groups, it may systematically reproduce those inequalities.

Consider, for example, an algorithm for predicting whether a particular person will commit a criminal offence. The first kind of discrimination could occur if the algorithm were trained on data drawn mostly on people from a particular geographic area. The algorithm would identify factors correlated with criminal offending for that group, but the correlation might be weaker, non-existent, or even negative for a different group, such that the algorithm produces worse outcomes when applied to the latter group. The second kind of discrimination could occur if the algorithm were trained on data which reflected the historical over-policing of black and minority ethnic communities.[[8]](#footnote-8) The algorithm could identify and incorporate an apparent correlation between criminal offending and race (or some other variable correlated with race, such as postcode), such that it is more likely to predict that people from those communities will commit offences in the future.

While the general risks of algorithmic discrimination are increasingly clear, it can be very difficult to establish that a specific algorithm is in fact discriminatory. This is particularly so for people affected by the government’s use of data-driven decision-making. People on the receiving end of such decisions will often lack access to the information (egsource code, training data, inputs and outputs, explanations) required to assess whether an algorithm is discriminatory, or lack the expertise and resources required to conduct such an assessment or engage someone else to do so.[[9]](#footnote-9)

This raises a dilemma for courts faced with public law challenges to potentially discriminatory algorithms. How should courts allocate the burden of testing for and proving whether a government algorithm is discriminatory, as between the government and the person affected? The England and Wales Court of Appeal squarely confronted this dilemma in its recent decision in *R (Bridges) v South Wales Police*.[[10]](#footnote-10) The decision provides welcome guidance on the duties of public bodies to identify and address algorithmic discrimination.

1. *Bridges*: discrimination in automated facial recognition technology

In *Bridges*, the plaintiff, Edward Bridges, claimed that the police’s use of automated facial recognition (AFR) technology was unlawful. One of Mr Bridges’ arguments was that the police had violated the public sector equality duty (PSED) under s 149(1) of the Equality Act 2010. The PSED requires public authorities to have ‘due regard’, among other things, to the need to eliminate discrimination.

In April 2017, as they were commencing a trial of their AFR system, the police had prepared an equality impact assessment, which they subsequently adduced as evidence of their compliance with the PSED. Mr Bridges argued that the impact assessment was inadequate, because it only considered whether the AFR system was directly discriminatory, and not whether it might be indirectly discriminatory against women or people of colour.

The Divisional Court rejected this argument at first instance.[[11]](#footnote-11) It found that Mr Bridges’ expert evidence addressed only the general risk of discrimination in AFR systems, rather than any ‘specific comment’ about the accuracy of the proprietary software licensed by the police.[[12]](#footnote-12) Mr Bridges did not establish that the police had any ‘specific reason’ to believe that their particular system might fare worse in identifying women or people of colour, or that their use of a ‘failsafe’—a human operator responsible for reviewing the system’s matches—was inadequate to address any risks of discrimination.[[13]](#footnote-13)

The Court of Appeal disagreed.[[14]](#footnote-14) It took a much more robust approach to the PSED itself, and found that the police failed to comply with that duty prior to or in the course of using the AFR system.[[15]](#footnote-15)

Turning first to the PSED itself, the Court found that it required the police to take reasonable steps to gather relevant information about the impact of their AFR system on people with protected characteristics.[[16]](#footnote-16) The Divisional Court had held that the police complied with the PSED because of the lack of any specific evidence that their system was discriminatory. But this got things the wrong way around.[[17]](#footnote-17) The PSED required the police to ‘proactively’ consider whether the technology might be discriminatory, including by making relevant enquiries, even where it appeared to be neutral.[[18]](#footnote-18)

The police cited three examples of how they had discharged the PSED: their use of a human failsafe; their own statistical analysis of the AFR system; and assurances from the private manufacturer of the system. The Court found that none of these was sufficient. First, as a matter of logic, the police’s substantive decision to use a failsafe could not satisfy their anterior, procedural obligation to gather information about whether the AFR system was discriminatory.[[19]](#footnote-19) The Court also doubted whether a failsafe would in fact address issues of discrimination, given that ‘human beings can also make mistakes.’[[20]](#footnote-20)

Second, the police’s own statistical analysis of the AFR system was flawed. In around November 2018, the police had analysed the system for evidence of bias.[[21]](#footnote-21) The analysis focused on the number of false positive alerts as a proportion of the total number of alerts generated by the system, during deployments over the previous 18 months.[[22]](#footnote-22) It found that there was no evidence of racial or gender bias.[[23]](#footnote-23) But this analysis was inadequate for two reasons. The first was that the police used the wrong metric. To determine whether the system was discriminatory, it was necessary to consider not just the number of alerts and false positive alerts, but also the full run of people actually captured by the system.[[24]](#footnote-24) The second reason was that the police officer conducting the analysis was ‘not an expert who [could] deal with the technical aspects of the software in this context.’[[25]](#footnote-25)

Third, the assurances from the private manufacturer of the AFR system were also inadequate. According to Mr Bridges’ expert, it was impossible to assess whether the system was discriminatory without examining the data used to train it.[[26]](#footnote-26) The police’s expert, a senior employee of the manufacturer, responded that the training data contained ‘roughly equal quantities of male and female faces’ and ‘a wide spectrum of different ethnicities,’ but declined to provide any further details on grounds of commercial confidentiality.[[27]](#footnote-27) The Court concluded that the police could not rely on these general assurances alone to discharge the PSED, a non-delegable duty.[[28]](#footnote-28) The police had ‘never sought to satisfy themselves, either directly or by way of independent verification,’ that their system was non-discriminatory.[[29]](#footnote-29)

Three important points emerge from *Bridges*. First, the PSED imposes a positive duty on public bodies to identify and address algorithmic discrimination. The Divisional Court’s reasoning set too low a bar for government in its use of algorithms. It permitted the government to blinker itself to credible risks of algorithmic discrimination, by simply not gathering further evidence. As the Court of Appeal found, this sat uneasily with the authorities on the PSED, which stress that it requires government to give ‘advance consideration’ to issues of discrimination before making a decision, so as to prevent governmental discrimination before it occurs.[[30]](#footnote-30) Prior to *Bridges*, the courts had indicated that the PSED could give rise to a duty of enquiry in particular cases, by application of the principles in *Secretary of State for Employment v Tameside Metropolitan Borough Council*.[[31]](#footnote-31) *Bridges* confirms that this duty of enquiry arises where the government proposes to use an algorithm to make decisions, at least where there is a credible risk of algorithmic discrimination. In such cases, the PSED places the burden of testing for and establishing algorithmic discrimination on government, rather than the people affected.

Second, the courts may closely scrutinise compliance with the PSED in this context. In general, a decision-maker is free to decide how and to what extent they enquire into the facts relevant to their decision, subject to review for legal unreasonableness.[[32]](#footnote-32) In *Bridges*, the Court adopted an arguably more stringent test: the police had ‘not done all that they reasonably could to fulfil the PSED.’[[33]](#footnote-33) The Court carefully considered both what information was required to effectively assess risks of algorithmic discrimination, and who was required to assess those risks. It found the police’s own statistical analysis inadequate on the first ground, and the manufacturer’s evidence inadequate on the second. In future, public bodies must rigorously examine whether the algorithms they propose to use are discriminatory, or engage an independent expert to do so on their behalf. It may not be enough for a public body to rely on its own, non-expert analysis, or on the general assurances of a manufacturer.

Third and relatedly, public bodies cannot escape these obligations by contracting them out. Many public bodies use private suppliers to build and manage their automated systems.[[34]](#footnote-34) *Bridges* makes clear that suppliers’ claims of commercial confidentiality cannot excuse public bodies from the requirements of the PSED.

1. A rigorous approach to algorithmic discrimination: international developments

Two recent decisions from other jurisdictions provide an instructive comparison with *Bridges*. Across a range of statutory contexts and legal systems, courts are placing the burden of proving algorithmic discrimination on public bodies, rather than the general public.

*Ewert v Canada*[[35]](#footnote-35) concerned a challenge to the Canadian Government’s use of statistical tools to assess prisoners’ psychopathy and risk of recidivism. The appellant, Jeffery Ewert, was Métis, an Indigenous group whose homeland stretches across Canada and the United States. He objected to the use of the tools because the government had a statutory duty to take ‘all reasonable steps’ to ensure that any information about a prisoner that it used was ‘accurate’, and there was a risk that the tools were culturally biased, because they were ‘developed for and validated by studies on predominantly non-Indigenous populations.’[[36]](#footnote-36)

Mr Ewert’s evidence was not dissimilar from that of Mr Bridges. The expert evidence indicated that ‘tests like the impugned tools are susceptible to “cross-cultural bias” or “variance”’, but no formal analysis had been done to confirm or eliminate that possibility.[[37]](#footnote-37)

The Supreme Court of Canada held that the government’s use of the tools was unlawful.[[38]](#footnote-38) The Court accepted that, as a practical matter, Mr Ewert needed to show that there was ‘some reason’ for the government to doubt the accuracy of the tools.[[39]](#footnote-39) But this was satisfied by the long-standing and credible ‘concerns regarding the possibility of psychological and actuarial tools exhibiting cultural bias.’[[40]](#footnote-40) There was no need for Mr Ewert to point to any specific, concrete error with the particular tools at issue. Given that it would have been eminently feasible for the government to conduct research into the tools, the Court concluded that the government’s failure to do so was unlawful.[[41]](#footnote-41) This conclusion was reinforced by the government’s statutory mandate to ensure that correctional policies respect ethnic and cultural differences and are responsive to the special needs of Indigenous persons.[[42]](#footnote-42)

Similarly, in *NJCM v The Netherlands*, the Hague District Court held that the Dutch Government’s automated system for detecting benefits fraud, known as ‘SyRI’, was incompatible with the right to private life under Article 8 of the European Convention on Human Rights.[[43]](#footnote-43) The Court found that SyRI seriously interfered with people’s privacy; it could process a very large amount of personal data, and it produced ‘risk reports’ which were available to public bodies, police and prosecutors.[[44]](#footnote-44) SyRI’s safeguards were also held to be inadequate. The government refused to disclose any specific information about how SyRI worked and the relevant legal framework did not ensure that SyRI’s data processing was limited by principles of necessity and proportionality.[[45]](#footnote-45)

An important factor in the Court’s decision was the risk of discrimination. The claimants, supported by the UN Special Rapporteur on extreme poverty and human rights,[[46]](#footnote-46) argued that there was a risk that SyRI was biased against people with particular characteristics, such as migrants or people of a particular socioeconomic status.[[47]](#footnote-47) The government’s secrecy around SyRI prevented the Court from reaching any conclusions on the nature and extent of this risk. The Court placed the burden of this uncertainty on the government, rather than the claimants. As the Court was unable to determine whether the government had ‘sufficiently neutralised’ the risk of discrimination, it took that risk into account in finding that SyRI violated the right to private life.[[48]](#footnote-48) In other words, once the claimants had raised a credible allegation of algorithmic discrimination, it was for the government to demonstrate that it had eliminated or mitigated any such risk.

1. Conclusion

*Bridges* raises at least two important issues for public law and algorithmic decision-making in government into the future. The first is the precise operation of the PSED in cases of algorithmic discrimination. In *Bridges*, there was clear expert evidence that discrimination was ‘a feature of common AFR systems.’[[49]](#footnote-49) More complex questions might arise where an algorithm is novel or there is otherwise no clear evidence of discrimination in systems of that kind. The courts might use the demanding standard of review applied in *Bridges*, requiring expert analysis of the system and its training data.Or they might use a less demanding standard of review, commensurate with the apparent level of risk posed by systems of that kind. The reasoning in *Bridges* and the PSED’s underlying rationale arguably support the first approach.

The second issue concerns proof of other kinds of public law error in algorithmic decision-making. The challenge of establishing that a government algorithm is discriminatory is part of a more general challenge: that of establishing that a government algorithm is unlawful.[[50]](#footnote-50) This is, for public law, an old problem in a new guise. Numerous public law doctrines help to ensure that claimants and courts can, in practice, establish whether the government has acted unlawfully. These include doctrines requiring the government to gather relevant information before making a decision,[[51]](#footnote-51) doctrines requiring the government to provide people affected and the courts with information about its decisions,[[52]](#footnote-52) and doctrines placing the burden on the government to prove certain facts when defending its decisions in court.[[53]](#footnote-53) The courts may need to develop these and other public law doctrines to ensure that the legal limits on algorithmic decision-making can be enforced.

The Court of Appeal’s decision in *Bridges* sends a strong signal to public bodies in the UK. The PSED requires such bodies to take positive steps to identify and address algorithmic discrimination, which the courts will scrupulously enforce. Public bodies cannot escape these duties by contracting them out. The decisions in *Ewert* and *NJCM* suggest that *Bridges* forms part of a broader trend: courts are placing the burden of testing and reviewing potentially discriminatory algorithms on government, rather than the general public. This is essential to ensure that public law norms, such as the PSED, remain effective in the era of algorithmic government.

Notes on contributor(s)

Jack Maxwell is Research Fellow in Public Law and Technology at the Public Law Project.

Joe Tomlinson is Senior Lecturer in Public Law at the University of York and Research Director at the Public Law Project.

1. \* j.maxwell@publiclawproject.org.uk [↑](#footnote-ref-1)
2. \*\* joe.tomlinson@york.ac.uk [↑](#footnote-ref-2)
3. Joe Tomlinson, ‘Quick and uneasy justice: An administrative justice analysis of the EU Settlement Scheme’ (*Public Law Project*, 2019) <publiclawproject.org.uk/wp-content/uploads/2019/07/Joe-Tomlinson-Quick-and-Uneasy-Justice-Full-Report-2019.pdf> accessed 4 September 2020. [↑](#footnote-ref-3)
4. Hannah Couchman, ‘Policing By Machine’ (*Liberty*, January 2019) <www.libertyhumanrights.org.uk/wp-content/uploads/2020/02/LIB-11-Predictive-Policing-Report-WEB.pdf> accessed 4 September 2020; Marion Oswald and others, ‘Algorithmic risk assessment policing models: lessons from the Durham HART model and “Experimental” proportionality’ (2018) 27 Information & Communications Technology Law 223; Silkie Carlo, Jennifer Krueckeberg, and Griff Ferris, ‘Face Off: The lawless growth of facial recognition in UK policing’ (*Big Brother Watch*, May 2018) <bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf> accessed 4 September 2020. [↑](#footnote-ref-4)
5. Joanna Redden, Lina Dencik, and Harry Warne, ‘Datafied child welfare services: unpacking politics, economics and power’ (2020) 41 Policy Studies 507;Sarah Marsh, ‘One in three councils using algorithms to make welfare decisions’ (*The Guardian*,15 October 2019) <www.theguardian.com/society/2019/oct/15/councils-using-algorithms-make-welfare-decisions-benefits> accessed 4 September 2020. [↑](#footnote-ref-5)
6. See generally Michael Rovatsos, Brent Mittelstadt, and Ansgar Koene, ‘Landscape Summary: Bias in Algorithmic Decision-Making’ (*Centre for Data Ethics and Innovation*, 19 July 2019) <assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\_data/file/819055/Landscape\_Summary\_-\_Bias\_in\_Algorithmic\_Decision-Making.pdf> accessed 4 September 2020. The literature tends to use the term ‘algorithmic discrimination’ and ‘algorithmic bias’ interchangeable. This note generally opts for the former, as it reflects the language of the Equality Act 2010 and the public sector equality duty (s 149(1)). [↑](#footnote-ref-6)
7. See Solon Barocas and Andrew D Selbst, ‘Big Data’s Disparate Impact’ (2016) 104 California Law Review 671, 677–93. [↑](#footnote-ref-7)
8. See, eg, Michael Shiner and others, ‘The Colour of Injustice: “Race”, drugs and law enforcement in England and Wales’(*Stopwatch* and *Release*, 2018) <eprints.lse.ac.uk/100751/1/TheColourOfInjustice.pdf> accessed 4 September 2020.  [↑](#footnote-ref-8)
9. See Jenna Burrell, ‘How the machine “thinks”: understanding opacity in machine learning algorithms’ (2016) 3 Big Data & Society1; Lilian Edwards and Michael Veale, ‘Slave to the Algorithm? Why a “right to an explanation” is probably not the remedy you are looking for’ (2017) 16 Duke Law & Technology Review 18. [↑](#footnote-ref-9)
10. [2020] EWCA Civ 1058 (England and Wales Court of Appeal (EWCA)) (*Bridges* (EWCA)). [↑](#footnote-ref-10)
11. *R (Bridges) v Chief Constable of South Wales* [2019] EWHC 2341 (Admin) (England and Wales High Court (EWHC)) [153]–[158] (Haddon-Cave LJ and Swift J) (*Bridges* (EWHC)). [↑](#footnote-ref-11)
12. ibid [153]. [↑](#footnote-ref-12)
13. ibid [156]–[157]. [↑](#footnote-ref-13)
14. *Bridges* (EWCA)(n 8) [163]–[202] (Sir Terence Etherton MR, Sharp P, and Singh LJ). [↑](#footnote-ref-14)
15. The Court also found that the police’s use of AFR technology was unlawful on two other bases: it was not in accordance with law for the purposes of art 8(2) of the European Convention on Human Rights, and consequently the police’s data protection impact assessment for the technology did not comply with the Data Protection Act 2018. See ibid [54]–[130], [145]–[154]. [↑](#footnote-ref-15)
16. *Bridges* (EWCA)(n 8) [182]. [↑](#footnote-ref-16)
17. ibid. [↑](#footnote-ref-17)
18. Karon Monaghan QC, *Equality Law* (2nd edn, Oxford University Press 2013) [16.06], quoted in ibid [178]. [↑](#footnote-ref-18)
19. ibid [185]. [↑](#footnote-ref-19)
20. ibid. [↑](#footnote-ref-20)
21. *Bridges* (EWHC)(n 9) [154]. [↑](#footnote-ref-21)
22. ibid. [↑](#footnote-ref-22)
23. *Bridges* (EWCA)(n 8) [186]–[190]. The police found a higher rate of false positive alerts for women than for men (82 per cent compared to 66 per cent), but concluded that this was due to two women on the police’s watchlist with ‘generic features that may match much more frequently.’ In relation to race, the police found that 98.5 per cent of false positive alerts were for ‘white north European’, and concluded that there was no racial bias. [↑](#footnote-ref-23)
24. ibid [191]. [↑](#footnote-ref-24)
25. ibid. [↑](#footnote-ref-25)
26. ibid [193], [197]–[198]. [↑](#footnote-ref-26)
27. ibid [196]. [↑](#footnote-ref-27)
28. ibid [199]. [↑](#footnote-ref-28)
29. ibid. [↑](#footnote-ref-29)
30. *Elias v Secretary of State for Defence* [2006] EWCA Civ 1293 (EWCA) [274] (Arden LJ), quoted in ibid [180]. [↑](#footnote-ref-30)
31. [1977] AC 1014, 1065 (Lord Diplock) (House of Lords (HL)). See, eg, *R (on the application of Hurley and Moore) v Secretary of State for Business Innovation & Skills* [2012] EWHC 201 (Admin) (EWHC) [89]–[90] (Elias LJ). [↑](#footnote-ref-31)
32. *R (on the application of Khatun) v London Borough of Newham* [2004] EWCA Civ 55 (EWCA) [35] (Laws LJ, Wilson J and Auld LJ agreeing); *R (on the application of Plantagenet Alliance) v Secretary of State for Justice* [2014] EWHC 1662 (Admin)(EWHC) [100] (Hallett LJ, Ouseley and Haddon-Cave JJ). [↑](#footnote-ref-32)
33. *Bridges* (EWCA)(n 8) [201]. [↑](#footnote-ref-33)
34. Committee on Standards in Public Life, *Artificial Intelligence and Public Standards: A Review by the Committee on Standards in Public Life* (February 2020) 49 <assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\_data/file/868284/Web\_Version\_AI\_and\_Public\_Standards.PDF> accessed 4 September 2020. [↑](#footnote-ref-34)
35. [2018] SCC 30 (Supreme Court of Canada). [↑](#footnote-ref-35)
36. ibid [3]–[18] (Wagner J). [↑](#footnote-ref-36)
37. ibid [13]–[14] (Wagner J). [↑](#footnote-ref-37)
38. ibid [28]–[67] (Wagner J). [↑](#footnote-ref-38)
39. ibid [47] (Wagner J). [↑](#footnote-ref-39)
40. ibid [49] (Wagner J). [↑](#footnote-ref-40)
41. ibid[50] (Wagner J) [↑](#footnote-ref-41)
42. ibid [51]–[66] (Wagner J) [↑](#footnote-ref-42)
43. C-09-550982-HA ZA 18-388 (English) (Hague District Court). [↑](#footnote-ref-43)
44. ibid [6.59], [6.60]–[6.65]. [↑](#footnote-ref-44)
45. ibid [6.80]–[6.106]. [↑](#footnote-ref-45)
46. Philip Alston, ‘Brief by the United Nations Special Rapporteur on extreme poverty and human rights as *Amicus Curiae* in the case of NJCM c.s./De Staat der Nederlander (SyRI) before the District Court of The Hague (case number: C/09/550982/ HA ZA 18/388)’ (*United Nations Special Rapporteur on extreme poverty and human rights*, 26 September 2019) <www.ohchr.org/Documents/Issues/Poverty/Amicusfinalversionsigned.pdf> accessed 25 March 2020. [↑](#footnote-ref-46)
47. *NJCM* (n 41) [6.91]–[6.95]. [↑](#footnote-ref-47)
48. ibid [6.93]–[6.95]. [↑](#footnote-ref-48)
49. *Bridges* (EWCA)(n 8) [193], [197], [199]. AFR systems are notoriously problematic in their treatment of women and people of colour. See, eg, Joy Buolamwini and Timnit Gebru, ‘Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification’ (2018) 81 Proceedings of Machine Learning Research 1, 1–15; Patrick Grother, Mei Ngan, and Kayee Hanaoka, ‘Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects’(*National Institute of Standards and Technology*, 2019) <nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf> accessed 7 September 2020. [↑](#footnote-ref-49)
50. See Joe Tomlinson, Katy Sheridan, and Adam Harkens, ‘Judicial Review Evidence in the Era of the Digital State’ (2020)Public Law (forthcoming). [↑](#footnote-ref-50)
51. See, eg, *Tameside* (n 29). See, in relation to algorithmic decision-making, Christopher Knight, ‘Automated Decision-making and Judicial Review’ (2020) Judicial Review (forthcoming). [↑](#footnote-ref-51)
52. See, eg, *R v Secretary of State for the Home Department, Ex p Doody* [1994] 1 AC 531, 565 (Lord Mustill) (HL); *R (on the application of Lumba) v Secretary of State for the Home Department* [2011] UKSC 12 (United Kingdom Supreme Court (UKSC)) [20]–[39] (Lord Phillips); *R (on the application of Hoareau) v Secretary of State for Foreign and Commonwealth Affairs* [2018] EWHC 1508 (Admin) (EWHC)[8]–[24] (Singh LJ). See, in relation to algorithmic decision-making, *R (on the application of Ames) v Lord Chancellor* [2018] EWHC 2250 (Admin) (EWHC). [↑](#footnote-ref-52)
53. See, in relation to the burden of proof under the Human Rights Act 1998, *Aguilar Quila v Secretary of State for Home Department* [2011] UKSC 45 (UKSC) [44] (Lord Wilson) [61] (Lady Hale); *R (on the application of Kiarie and Byndloss) v Secretary of State for the Home Department* [2017] UKSC 42 (UKSC) [78] (Lord Wilson, Lady Hale, Lord Hodge and Lord Toulson agreeing). [↑](#footnote-ref-53)