



Neutral Citation Number: [2025] EWHC 146 (ADMIN)

Case No: AC-2023-BHM-000236

IN THE HIGH COURT OF JUSTICE
KING'S BENCH DIVISION
ADMINISTRATIVE COURT

Birmingham Civil and Family Justice Centre
33 Bull Street, Birmingham, B4 6DS

Date: 29/01/2025

Before :

MRS JUSTICE STACEY

Between :

HEATHER PETO
- and -
THE INFORMATION COMMISSIONER

Claimant

Defendant

Ms Peto acting for herself as claimant litigant in person
Mr Leo Davidson (of counsel) for the Defendant.

Hearing date: 13 December 2024

Approved Judgment

This judgment was handed down remotely at 10.30am on 29th January 2025 by circulation to the parties or their representatives by e-mail and by release to the National Archives.

.....
MRS JUSTICE STACEY

Mrs Justice Stacey:

1. This matter came before the Court on the claimant’s renewed oral application following the refusal of permission to apply for judicial review by the single judge, Eyre J, and his provisional costs order made on the papers (“the Order”). There were also a number of other applications before the court which would, or might, become relevant if permission is granted. It was not possible to conclude the hearing and give judgment in the time allotted for the hearing since there was much that both parties wanted to raise orally and nor was it possible to allow the case simply to run on given the rest of the day’s list, so to avoid curtailing the parties’ oral submissions, judgment was reserved and the parties informed that no further written submissions would be permitted in what was hoped would be a short time between the end of the hearing and the handing down of this judgment.
2. In a claim form issued on 14 November 2023 the claimant seeks to challenge two matters. The first is what is said to be the continuing threat by the defendant, the Information Commissioner, “the ICO” or the defendant) to prosecute the claimant under s.170 Data Protection Act 2018 (“the Act”) if she were to inform 120 others of breaches of their GDPR rights and the second is the alleged failure of the ICO in a decision dated 9 August 2023 to enforce GDPR by failing to prosecute the data controller for breach of the rights of the 120 others and the ICO’s failure to inform the 120 others of the fact of the breaches of their rights. The provisions of s.170 and s.173 are set out in the annex to this judgment.
3. In the Order permission to apply for the first element, the challenge to the maintenance of the warning that her proposed or intended actions might be a breach of the Act was refused since the warning was an expression of the defendant’s view that such actions might be an offence. There was no basis that this was anything other than a genuine expression of the position as understood by the defendant. Whether an offence will be committed if the claimant acts in the way suggested will depend upon the particular circumstances when the action is taken and on the analysis of her actual conduct in light of the terms of the Act. Until such action is taken and the circumstances established the question of the lawfulness of the actions is not only academic but incapable of a definitive answer (see [5]-[8] of the Order). It had no reasonable prospects of success.
4. The second element of the claim was noted in the Order to be in time, but it also had no reasonable prospects of success. The question of whether there is sufficient evidence to justify a prosecution and whether a prosecution is merited are matters for the judgment of the defendant as a specialist body. It will only be in the clearest of cases that it will be appropriate for the court to conclude that the defendant’s decision not to prosecute was irrational or unlawful. In this case it could not be said that the ICO had adopted an unlawful policy of not enforcing the Act. Instead it had concluded that there was insufficient evidence to warrant a prosecution in the circumstances of this case. There was no prospect of showing that there was evidence which was so compelling that the decision not to prosecute was outside the wide range of the ICO’s discretion. The Order declined the defendant’s application to certify the claim as being totally without merit: although it had no real prospect of success, it could no be said that there was no rational basis on which it could succeed. On a summary assessment the Judge made a provisional order that the claimant pay the defendant’s costs of £1,620.

Background facts

5. The claimant is a member of the Labour Party and was re-elected as co-chair of a group within the Labour Party called LGBT+ Labour and sat as the group's representative on the sub-committee for Equalities of the Labour Party's ruling body, the National Executive Council (NEC), under its rules and constitution. Both LGBT+ Labour and the Labour Party itself are data controllers under the GDPR.
6. Between 2012-2020 LGBT+ Labour ran a private and confidential forum for trans activists called the trans forum ("the Trans Forum") which had 120 members including the claimant as at 2020. Membership of the Trans Forum was vetted to ensure that potential members were trans and were not going to disclose other members' identity or comments. It was intended to be a safe space for its members to discuss matters freely, openly and in confidence and to advance the policy agenda on trans issues within the Labour Party.
7. The claimant states that in breach of data protection obligations data from the Trans Forum was disclosed widely within both LGBT+ Labour and the Labour Party in December 2020 in an email of 2 December 2020, including the identity of the members of the Trans Forum and their trans status, that in some parts the contents of the information on the Trans Forum had been falsified and in others taken out of context to create a misleading impression about the activities and views of the group, and that this information and data was then used to threaten disciplinary proceedings and sanctions against the 120 Trans Forum members for breach of the Labour Party rule book. When the claimant became aware of the breach as co chair of LGBT+ Labour she considered herself to be a data controller and commenced an investigation into the breach. On 8 December 2020 she emailed the sender of the email of 2 December 2020 and asked for an explanation of what had happened. However before she obtained an answer the claimant was removed from the data breach investigation at a meeting of LGBT+ Labour on 12 December 2020. She resigned as co-chair on 28 January 2021 alleging discrimination by the Labour Party and LGBT+ Labour on the grounds of the protected status of gender reassignment and victimisation contrary to s.27 Equality Act 2010 relying on her email of 8 December 2020 to the sender of the 2 December 2020 email as a protected act, as a result of which she asserted that she was being subjected to a detriment.
8. The claimant has made a number of Subject Access Requests (SAR) since then which she does not consider have been satisfactorily responded to by LGBT+ Labour. She is also aware that one of the other 120 members of the now disbanded Trans Forum, referred to as DS7, also made a SAR since she received a copy of the SAR on 25 January 2021 whilst she was still co-chair of LGBT+ Labour. She believes that DS7 received a false or inaccurate response to their SAR and was not informed of the fact of the data breach by the email of 2 December 2020.
9. Concerned that there was something of a Catch-22 – that she was aware of the data breach of the email of 2 December 2020 because of her then position as co-chair of LGBT+ Labour but was also aware that the 120 Trans Forum members had not been informed by the data controllers – either by her when she was a data controller prior to her resignation as co-chair of LGBT+ Labour, or by her successors, so that the others in the forum would not know of the breach, the claimant brought the matter to the attention of the ICO in what she described as whistleblowing letters in May 2021 and on 10 June 2021. She made what she called protected disclosures that two data controllers were concealing from the ICO and victims offences under ss. 170(1) and

173 of the Act; that there were severe GDPR breaches and unlawful processing of stolen and falsified data to victimise and discriminate against the 120 Labour Party members who shared the s.7 Equality Act 2010 protected characteristic of gender reassignment. In the autumn of 2021 the claimant began collecting data in order to tell the 120 Trans Forum members who's data rights she thought had been breached, starting with the 8 who had been singled out for particular criticism and allegations by LGBT+ Labour and possibly the wider Labour Party for their comments and contributions to the chat in the Trans Forum.

10. On 30 November 2021 the ICO case worker assigned to the complaint updated the claimant on progress to say that he intended to have a meeting with the Labour Party, would raise the ICO's concerns with them directly and would write with a further update. In response to a further question the claimant had asked the case worker said this:

“Finally, you have raised concerns regarding information you came across while you were co-chair of LGBT+ Labour. I note that you have asked whether you are able to discuss matters relating to potential data breaches with the individuals involved. I would advise that you should raise this with LGBT+ Labour in the first instance as this could potentially be a section 170 offence under the Data Protection Act 2018. This is because disclosing information relating to personal data without the consent of the data controller could be considered an offence under s.170”

11. The claimant pushed back against the letter as she believed that the defences set out in both s.170(2) and (3) of the Act would apply if she were to obtain or disclose personal data without the consent of the controller and she continued to correspond at some length with the ICO in a manner which is at times confusing. She also pushed for the ICO to take prosecutorial action against the Labour Party and LGBT+ Labour for the breaches that she had reported to them.
12. On 17 July 2023 the ICO decided that the evidence that the claimant had provided to it “does not clearly support your s.170/173 concerns.” The claimant responded challenging the decision and a review was undertaken by the Criminal Investigations Team. On 9 August 2023 the Lead Case Officer at the ICO emailed the claimant to explain that after her letter of 21 July 2023 and further consideration by the Criminal Investigations team the conclusion was that there was insufficient evidence to substantiate a s.173 offence and the ICO was taking no further action on the matter. She was assured that all the necessary steps to investigate and refer the complain had been taken and if she wished to pursue the matter further, she had the option of pursuing the matter through the courts if she wished.
13. Following further correspondence, on 30 October 2024 the ICO confirmed once again that it was taking no further action in relation to her s.170/173 concerns. As to the claimant's concern about the risk to her of being prosecuted, the ICO repeated the original observations made nigh on 2 years earlier by the Case Worker on 30 November 2021. In a letter from the Senior Policy Officer the claimant was told that the advice provided in 2021 was appropriate and the ICO would not be taking any further action but a formal case or service review could be arranged if she so wished.

14. Judicial review proceedings ensued in a claim form issued on 14 November 2023.

The renewal application

15. In her renewal application, the claimant does not consider that the paper decision had taken sufficient account of the GDPR and ECHR rights of the 120 members of the Trans Forum who have the protected characteristic of gender reassignment. The Order had failed to address the points that the claimant had raised about breaches of GDPR and/or ECHR/Human Rights Act 1998 (“HRA 1998”) and had not addressed the Public Sector Equality Duty which applied to the ICO, or the Public Interest Disclosure Act 1998 (“PIDA 1998”). She asserted that she had status under s.7 HRA 1998 as the ICO had violated her Article 6 & 8 rights as well as those of other 120 transgender victims without proportionate justification.
16. The claimant notes she has standing under s.7 HRA 1998 – she claims that a public authority has acted (or proposes to act) in a way which is made unlawful by s.6 and she is, or would be a victim of the unlawful act both for herself and in a representative capacity of the other 119 members of the Trans Forum, which was not referred to in the Order. Nor had the Order addressed the claimant’s complaint about the defendant’s breach of the duty of candour.
17. She reiterated her deep anxiety and concern at the threat of prosecution. She considered that she faced an intolerable Catch-22: she was aware of the breaches that she believed had occurred, believed that the data controllers had failed to inform the 120 Trans Forum members of the data protection breaches, therefore those others did not know about it in order to complain about it or report it, and the one who had raised an SAR – DS7 - had received an unsatisfactory, and in the claimant’s view false, response and was still none the wiser. Yet the claimant dare not tell the others for fear of being prosecuted under s.170 when to her mind she would have a cast iron defence if she were to do so. Meanwhile the ICO had decided to take no action against the LGBT+ Labour or the Labour Party for what the claimant considered were egregious breaches, including falsifying data which had had real and harmful consequence for the individuals within the Labour Party.

Analysis and conclusions

18. The difficulty for the claimant with the additional points raised by her in her renewal application is that they do not address the fundamental difficulties identified in the Order which led to the conclusion that there were no reasonable prospects of success in either element of the claim. The starting point must be an identifiable cause of action with a realistic prospect of success.
19. In the first element, the claimant’s request was for a commitment that she would not be prosecuted in a hypothetical and future fact sensitive situation. The provisions of s.170 of the Act are set out in the annex to the judgment and, as can be seen, the section is complex and highly fact and context sensitive as to when and whether a prima facie offence is committed and how the various defences available might apply in any specific circumstance. Without knowing all the facts – most of which have not yet happened, and others which are no controversial and contested, it would not be possible for the ICO to say with confidence what view it might take in what is an imaginary world with many, many different permutations of what the circumstances and facts

might be at that future time. The court does not decide hypothetical or academic issues and nor could the ICO be expected to do so, particularly when they had only the claimant's version of events (see *R(Rusbridger) v AG* [2003] UKHL 38 at [35] and [56]) and when the decision will be fact sensitive (*R(Zoolife International Ltd) v SSEFRA* [2007] EWHC 2995 (Admin) at [36]). I also note in passing that the Order did address the HRA and Equality Act 2010 issues in the penultimate sentence of paragraph 10.

20. So there was no need for the Order to address such matters as the claimant's locus. Indeed her standing is not in dispute in this case –which is why it was not necessary for it to be dealt with in the Order, since it did not form part of the reason for refusal of permission, which was the lack of underlying merit. Similarly there was no need for the Order to engage in detail with the ECHR/HRA arguments in detail as there are no realistic prospects of succeeding in a claim that the ICO should have given the claimant the reassurance that she sought in anticipation of what she might do.
21. The response the claimant received to her question could not be characterised as a threat, but a noting of the fact of the section and the uncontroversial statement that if the claimant were to obtain or disclose personal data without the consent of the controller it *might* be an offence under s.170. It is a very far removed situation from, and factually very different to, any of the case law cited by the claimant in support of this element of her claim.
22. There is therefore no decision capable of being challenged, but if the 30 November 2021 email could be said to be such a decision, the claim is lodged far too late and is over 18 months out of time as the 30 October 2023 email was carefully worded so as not to constitute a fresh decision.
23. As to ground or element two – the ICO's decision not to prosecute the Labour Party or LGBT+ Labour for breaches of s.170 and/or 173 of the Act – the Order is criticised for not addressing the duty of candour. As I understand it the argument runs thus: the claimant was told only that there was insufficient evidence to prosecute which she challenges as an inadequate explanation in itself and, now that she has lodged proceedings the explanation breaches the obligation to provide a brief summary of reasoning underlying the measures in respect of which permission for judicial review is sought in the summary grounds of defence (Administrative Court Guide 2024 15.3.3).
24. Here too there may be time limit issues, notwithstanding that the Order considered on first blush that the claim was in time. Time may well have started running from 17 July 2023, not 9 August 2023, and promptness may have required the claimant to act much, much sooner in 2021 - given the short statutory time limits for prosecuting breaches of s.170 and 173, but I will leave that aside for the moment and consider the merits of the claim.
25. The reason why the Judge found that there was no realistic prospect of success set out in the Order is that the question of whether there is sufficient evidence to justify a prosecution and whether a prosecution is merited are matters for the judgment of the defendant as a specialist body. As per *R(Corner House and others) v Director of the Serious Fraud Office* [2008] UKHL 60 a body such as the ICO (like the Serious Fraud Office (as it then was)) is entrusted by Parliament with discretionary powers to investigate suspected data protection offences and the power and discretion to prosecute

such cases. The ICO is an independent, professional service, a specialist body in a specialist area with expertise and experience in the field. Although its decisions are not immune from review by the courts, the authorities make plain that only in highly exceptional circumstances will the court disturb the decisions of an independent prosecutor and investigator (at [30] per Lord Bingham).

26. Whilst there were many, many pages of emails and letters and documents submitted by the claimant in support of her application, this dispute is, at heart, an internal dispute within the Labour Party and the power struggles between various factions and special interest groups, as is entirely normal and natural in any political organisation (and indeed many organisations of every shape, style and type). I could not identify any evidence, from the claimant either when considered singly or when looked at as a whole, that indicated that there were any “highly exceptional circumstances” in this case that would enable this court to consider there was a realistic prospect of showing that the ICO had acted outside the wide range of its discretion when deciding not to prosecute.
27. It also follows that in the absence of such compelling evidence the defendant is not obliged to provide reasons of why the evidence was considered insufficient. Nor is there a realistic prospect of arguing that there has been a breach of the duty of candour when there is a lack of evidence to support the judicial review challenge to the defendant’s decision not to prosecute the Labour Party or LGBT+ Labour.
28. Permission to apply for judicial review is therefore refused. It is therefore not necessary to consider the other applications, such as a costs capping order.
29. I have considered also the defendant’s renewed application for the case to be certified as being totally without merit. Whilst I agree that ground one is bound to fail as being both out of time and on the substantive merits, ground two is more borderline. The defendant could have been more forthcoming about why the evidence was insufficient and explained its position a little. I agree with Eyre J that although the argument has no realistic prospect of success, it is not quite so hopeless as to merit certification as TWM.
30. The claimant explained that a motivator for her in bringing this litigation was her desire for the 120 Trans Forum members to be aware that their data rights may have been breached and she wanted to be able to bring it to their attention. It may be of some comfort for the claimant to know that it may be that through this judgment those other 119 people (and only they will know if they were members of the Trans Forum at the time) will become aware of the possibility that their rights were infringed.
31. As to the costs order, I find that the defendant is entitled to its costs in preparing and lodging the acknowledgement of service and summary grounds of defence. I know how long I have spent reading and understanding the papers and how very time consuming it has been. The costs claimed were reasonable and proportionate on a summary assessment. I have taken note of the claimant’s limited means and health conditions, but find that the amount claimed is entirely justified and reasonable for the amount of work that must have been involved by counsel. The claimant has been spared by their being no claim for solicitors’ costs. The defendant has not asked and will not be compensated for its attendance at the oral renewal hearing for which it will have incurred costs. But in deference to the claimant’s health and limited means and in order for her to have time to agree a costs payment arrangement with the defendant I order

the claimant to pay the sum of £1,620 within the longer period of 56 days from date of service of the order consequent on this judgment.

Annex

Statutory provisions Data Protection Act 2018

s. 170 Unlawful obtaining etc of personal data

(1) It is an offence for a person knowingly or recklessly—

- (a) to obtain or disclose personal data without the consent of the controller,
- (b) to procure the disclosure of personal data to another person without the consent of the controller, or
- (c) after obtaining personal data, to retain it without the consent of the person who was the controller in relation to the personal data when it was obtained.

(2) It is a defence for a person charged with an offence under subsection (1) to prove that the obtaining, disclosing, procuring or retaining—

- (a) was necessary for the purposes of preventing or detecting crime,
- (b) was required or authorised by an enactment, by a rule of law or by the order of a court or tribunal, or
- (c) in the particular circumstances, was justified as being in the public interest.

(2) It is also a defence for a person charged with an offence under subsection (1) to prove that—

- (a) the person acted in the reasonable belief that the person had a legal right to do the obtaining, disclosing, procuring or retaining,
- (b) the person acted in the reasonable belief that the person would have had the consent of the controller if the controller had known about the obtaining, disclosing, procuring or retaining and the circumstances of it, or
- (c) the person acted—
 - (i) for the special purposes,
 - (ii) with a view to the publication by a person of any journalistic, academic, artistic or literary material, and
 - (iii) in the reasonable belief that in the particular circumstances the obtaining, disclosing, procuring or retaining was justified as being in the public interest.

s.173 Alteration etc of personal data to prevent disclosure to data subject

(1) Subsection (3) applies where—

- (a) a request has been made in exercise of a data subject access right, and

- (b) the person making the request would have been entitled to receive information in response to that request.
- (2) In this section, “data subject access right” means a right under—
- (a) Article 15 of the [F1UK GDPR] (right of access by the data subject);
 - (b) Article 20 of the [F2UK GDPR] (right to data portability);
 - (c) section 45 of this Act (law enforcement processing: right of access by the data subject);
 - (d) section 94 of this Act (intelligence services processing: right of access by the data subject).
- (3) It is an offence for a person listed in subsection (4) to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure of all or part of the information that the person making the request would have been entitled to receive.
- (4) Those persons are—
- (a) the controller, and
 - (b) a person who is employed by the controller, an officer of the controller or subject to the direction of the controller.
- (5) It is a defence for a person charged with an offence under subsection (3) to prove that—
- (a) the alteration, defacing, blocking, erasure, destruction or concealment of the information would have occurred in the absence of a request made in exercise of a data subject access right, or
 - (b) the person acted in the reasonable belief that the person making the request was not entitled to receive the information in response to the request.