Neutral Citation Number: [2018] EWCA Civ 70

Case No: C1/2015/2612 & 2613

IN THE COURT OF APPEAL (CIVIL DIVISION)
ON APPEAL FROM THE HIGH COURT OF JUSTICE
QUEEN'S BENCH DIVISION, DIVISIONAL COURT
LORD JUSTICE BEAN AND MR JUSTICE COLLINS
Cases No. CO/3655/2014; CO/3667/2014; CO/3794/2014

Royal Courts of Justice
Strand, London, WC2A 2LL

Date: 30/01/2018

Before:

SIR GEOFFREY VOS, CHANCELLOR OF THE HIGH COURT
LORD JUSTICE PATTEN
and
LORD LLOYD JONES

Between:

SECRETARY OF STATE FOR THE HOME DEPARTMENT

Appellant

- and -

(1) TOM WATSON MP
(2) PETER BRICE
(3) GEOFFREY LEWIS

Respondents

- and -

(1) OPEN RIGHTS GROUP
(2) PRIVACY INTERNATIONAL
(3) THE LAW SOCIETY OF ENGLAND AND WALES

Interveners

James Eadie QC, Gerry Facenna QC and **Michael Armitage** (instructed by Government Legal Department) for the **Appellant**
Ben Jaffey QC and **Iain Steele** (instructed by Liberty) for the **First Respondent**
Richard Drabble QC, Ramby De Mello and **Azeem Suterwalla** (instructed by Bhatia Best Solicitors) for the **Second and Third Respondents**
Jessica Simor QC and **Ravi Mehta** (instructed by Deighton Pierce Glynn) for the First and Second **Interveners**

Hearing date: 8 December 2017

JUDGMENT

Lord Lloyd-Jones:

1. On 20 November 2015 this court gave judgment in these proceedings ([2015] EWCA Civ 1185) referring preliminary issues to the Court of Justice to the European Union ("CJEU"). We refer to that judgment for the history of the proceedings and the issues in the domestic proceedings. The principal purpose of the reference was to obtain clarification of the judgment of the CJEU in Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Limited v Minister for Communications, Marine and Natural Resources & Others* and *Seitlinger and Others* delivered on 8 April 2014 ("Digital Rights Ireland Limited"). We referred the following questions.

> "1. Does the judgment of the Court of Justice in Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* and *Seitlinger*, ECLI:EU:C:2014:238 ("*Digital Rights Ireland*") (including, in particular, paras 60-62 thereof) lay down mandatory requirements of EU law applicable to a Member State's domestic regime governing access to data retained in accordance with national legislation, in order to comply with Article 7 and 8 of the EU Charter ("the EU Charter")?
>
> 2. Does the judgment of the Court of Justice in *Digital Rights Ireland* expand the scope of Articles 7 and/or 8 of the EU Charter beyond that of Article 8 of the European Convention on Human Rights ("ECHR") as established in the jurisprudence of the European Court of Human Rights ("ECtHR")?"

In our judgment of 20 November 2015 we stated (at [118]) that we considered that the answers to these questions of EU law were not clear and were necessary in order for us to give judgment in these proceedings.

2. The President of the CJEU granted an application that the reference be expedited and that it be joined to the reference made by the Stockholm Administrative Court of Appeals then pending as Case C-203/15 *Tele2 Sverige AB*.

3. Following a hearing on 12 April 2016, the Grand Chamber of the CJEU gave judgment on 21 December 2016. The dispositif reads as follows:-

> "1. Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union, must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication.
>
> 2. Article 15(1) of Directive 2002/58, as amended by Directive 2009/136 read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights must be interpreted as precluding

> national legislation governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime, where access is not subject to prior review of a court or an independent administrative authority, and where there is no requirement that the data concerned should be retained within the European Union.
>
> 3. The second question referred by the Court of Appeal (England & Wales) (Civil Division) is inadmissible."

4. It appears that the first paragraph of the dispositif reflects the language of the Swedish legislation which was the subject of the reference by the Swedish court, whereas paragraphs 2 and 3 of the dispositif reflect the questions referred by this court.

5. Following the handing down of the judgment of the CJEU, a considerable delay occurred before the matter was listed before this court for further hearing. At the prompting of the court it was listed for hearing on 7 June 2017 but that hearing was vacated because of the non-availability of certain counsel. The case has now been relisted for hearing before us.

6. There have been several developments since the judgment of the CJEU.

   (1) Sections 1 and 2 of the Data Retention and Investigatory Powers Act 2014 ("DRIPA") were repealed on 30 December 2016.

   (2) The legislation which has replaced the data retention arrangements under DRIPA, i.e. Part 4 of the Investigatory Powers Act 2016, is itself the subject of a judicial review claim brought by Liberty. This includes a challenge to the 2016 Act on grounds of non-compliance with the CJEU's judgment in the present case. Permission to apply for judicial review has been granted and a substantive hearing of the claim is due to be heard in the Administrative Court on 27 and 28 February 2018.

   (3) In proceedings brought by Privacy International against the Secretary of State for Foreign and Commonwealth Affairs and others the Investigatory Powers Tribunal ("the IPT") on 8 September 2017 made a further reference to the CJEU seeking, inter alia, to clarify the extent to which, if at all, the requirements set out in the CJEU's judgment in the present case apply in a national security context. (Judgment of Investigatory Powers Tribunal UKIPTrib IPT_15_110_CH). The questions referred are as follows:-
   "In circumstances where:

   > a. the SIAs' capabilities to use BCD supplied to them are essential to the protection of the national security of the United Kingdom, including in the fields of counter-terrorism, counter-espionage and counter-nuclear proliferation;
   >
   > b. a fundamental feature of the SIAs' use of the BCD is to discover previously unknown threats to national security by means of non-targeted bulk techniques which are reliant upon the aggregation of the BCD in one place. Its principal utility lies in swift target identification and development, as well as providing a basis for action in the face of imminent threat;
   >
   > c. the provider of an electronic communications network is not thereafter required to retain the BCD (beyond the period of

their ordinary business requirements), which is retained by the State (the SIAs) alone;

d. the national court has found (subject to certain reserved issues) that the safeguards surrounding the use of BCD by the SIAs are consistent with the requirements of the ECHR; and

e. the national court has found that the imposition of the requirements specified in §§119-125 of the judgment of the Grand Chamber in joined cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post-och telestyrelsen* and *Secretary of State for the Home Department v Watson and Others* (ECLI:EU:C:2016:970) *('the Watson* Requirements'), if applicable, would frustrate the measures taken to safeguard national security by the SIAs, and thereby put the national security of the United Kingdom at risk;

1. Having regard to Article 4 TEU and Article 1(3) of Directive 2002/58/EC on privacy and electronic communications (the "e-Privacy Directive"), does a requirement in a direction by a Secretary of State to a provider of an electronic communications network that it must provide bulk communications data to the Security and Intelligence Agencies ('SIAs') of a Member State fall within the scope of Union law and of the e-Privacy Directive?

2. If the answer to Question (1) is 'yes', do any of the *Watson* Requirements, or any other requirements in addition to those imposed by the ECHR, apply to such a direction by a Secretary of State? And, if so, how and to what extent do those requirements apply, taking into account the essential necessity of the SIAs to use bulk acquisition and automated processing techniques to protect national security and the extent to which such capabilities, if otherwise compliant with the ECHR, may be critically impeded by the imposition of such requirements?"

(4) On 30 November 2017 the Secretary of State published a consultation document and proposed amendments to the Investigatory Powers Act 2016 which are intended to address the judgment of the CJEU in the present proceedings. The consultation and proposed amendments deal, inter alia, with the restriction, in the context of fighting crime, to "serious crime", the need for prior review by a court or an independent administrative authority for access to retained data, ex-post facto notification and the issue of retention of retained communications data within the EU.

7. It is now for this court to seek to apply the decision of the CJEU to the challenge brought against DRIPA in the national proceedings. As Mr Jaffey QC, on behalf of the First Respondent, pointed out in the course of his oral submissions, the fact that DRIPA has now been repealed does not make this a pointless exercise. Nevertheless, I regret to say that the task now facing this court is far from easy in view of the fact that the preliminary ruling from the CJEU is lacking in clarity. This is apparent from the disputes between the parties before us as to its effect and from the fact that it has already given rise to a further reference by the IPT.

8. We have heard competing submissions as to whether, in these circumstances, it is appropriate for this court to grant declaratory relief and, if so, what form such relief should take. We note

that the Divisional Court granted declaratory relief and were this court simply to dismiss the appeal of the Secretary of State without more, those declarations would stand. No party before us has suggested that this would be a suitable disposal.

9. It is common-ground amongst the parties before us that the judgment of the CJEU establishes, at the very least, that where the purpose is the prevention, investigation, detection and prosecution of criminal offences:-

(1) access to and use of retained communications data should be restricted to the objective of fighting serious crime; and
(2) access to retained data should be dependent on a prior review by a court or an independent administrative body.

I consider that this is correct.

10. Article 15(1) of Directive 2002/58/EC permits Member States to adopt legislative measures to restrict the scope of the rights and obligations of the Directive "when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection, and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC". It provides that, to that end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on those grounds. The reference made by the IPT raises squarely the question whether the judgment of the CJEU in the present case and, in particular, the mandatory requirements identified in that judgment ("the *Watson* requirements") apply where the purpose is that of national security. (See the judgment of the Investigatory Powers Tribunal at paragraphs 23 and 54.) The IPT stated at paragraph 69 of its judgment making the reference:-

> "We have carefully considered the evidence before us, both from the Claimant and the Respondents, and we are persuaded that if the *Watson* requirements do apply to measures taken to safeguard national security, in particular the [Bulk Communications Data] regime, they would frustrate them and put the national security of the United Kingdom, and, it may be, other Member States, at risk. It is to be hoped that, whether by reconsideration, or clarification, of paragraph 119 of the Judgment, or otherwise, the Grand Chamber will take the opportunity to consider whether any further statement than that the safeguarding provisions of the ECHR should apply is required."

11. On behalf of the Secretary of State, Mr Eadie QC submits that the reasoning of the CJEU, in particular at paragraphs 102, 103, 108, 110-112, 119-120 and 125, is limited to the purpose of fighting crime. He makes the point that, apart from a reference to public security at paragraph 111, the only reference in the judgment of the CJEU to national security is at paragraph 119. In that regard, he also refers to the terms of the dispositif. That submission is not accepted by the respondents or the interveners.

12. However, it is not necessary for this court to come to a conclusion on that point because the respondents agree that, in order to avoid pre-empting matters which will have to be considered on the reference by the IPT, any declaratory relief granted in these proceedings should be expressly limited to the application of the *Watson* requirements to cases concerned with fighting crime. (I should point out that Ms Simor QC who appeared on behalf of the First and Second Interveners did not agree to such a course but expressly stated that she would not seek to persuade us to take a different course). I consider that this is the most appropriate course. In view of the controversy over this issue before the IPT and the fact that

it is now the subject of a further reference to the CJEU, it would not be appropriate for this court to seek to resolve the issue. Accordingly, any declaratory relief should, in my view, be expressly limited to the application of DRIPA to fighting crime.

13. In these circumstances I consider that it is appropriate to grant declaratory relief, limited to the context of the prevention, investigation, detection and prosecution of criminal offences, to the effect that DRIPA was inconsistent with EU law to the extent that it permitted access to retained data, where the objective pursued by that access was not restricted solely to fighting serious crime, or where access was not subject to prior review by a court or an independent administrative authority.

Retention in the EU

14. In these proceedings, the First Respondent contends that DRIPA does not contain adequate safeguards against communications data leaving the European Union. It is submitted that the Divisional Court rightly identified that domestic law is deficient in this respect but wrongly concluded that on a proper interpretation of *Digital Rights Ireland* it is not necessary for restrictions on passing on information about communications data outside the EU to be embodied in statute. The First Respondent submits that the Divisional Court should have held that the deficiency in domestic law was a further reason for holding that section 1 of DRIPA is inconsistent with EU law (see Respondent's skeleton argument before the Court of Appeal, paragraphs 75, 76). Accordingly, the First Respondent issued a Respondent's Notice to that effect. I understand that this is also the position of the Second and Third Respondents.

15. The dispositif of the judgment of the CJEU in the present case expressly refers to such a requirement stating that national legislation governing the protection and security of traffic and location data is precluded "where there is no requirement that the data concerned should be retained within the European Union". This may be taken as reflecting paragraph 122 of the judgment where the Court states that the providers of electronic communications services must, in order to ensure the full integrity and confidentiality of data, guarantee a particularly high level of protection and security by means of appropriate technical and organisational measures. It then states:

> "In particular, the national legislation must make provision for the data to be retained within the European Union and for the irreversible destruction of the data at the end of the data retention period ..."

16. On this basis we are urged by the Respondents and the Interveners to grant declaratory relief to that effect.

17. Mr Eadie, however, submits that there is a deep uncertainty as to the precise meaning and scope of these passages in the judgment of the CJEU. On their face, they appear to impose an absolute, unconditional requirement. By contrast the argument before the national courts in these proceedings has, to date, been on the basis that there was a lack of adequate safeguards. Furthermore, it is clear from the IPT judgment that it is the position of Privacy International, the claimant in those proceedings, that the obligation is not an absolute one. At paragraph 65 of its judgment the IPT records the submission of Privacy International in those proceedings.

> "However, the Claimant submits that it is not an absolute bar, because of the interpolation of paragraph 123 between paragraphs 122 and 125. That paragraph provides for there to be a review by an independent authority of compliance with the level of protection guaranteed by EU law, and Mr. De la Mare submitted that, by virtue of the reference to Article 8(3) of the Charter, this was to be seen as

> an independent authority supervising the transfer of data out of the European Union, thus making the bar not absolute."

I also note that it was common-ground among the parties before the IPT that there was uncertainty as to the scope of this obligation.

18. The IPT also referred to an alternative submission of the claimant in those proceedings that the requirement is only for the data itself to remain in the European Union and not the product of the data. The Tribunal, while noting that, if that is so, it is less of a restriction, observed (at paragraph 65) that the reference in paragraph 123 to a potential claim by a person "seeking the protection of their data" would not appear to support this reading. The Tribunal went on to observe (at paragraph 67) that a requirement imposing an absolute bar would appear to be in clear conflict with earlier decisions of the CJEU in Joined Cases C-317/04& C-318/04 *Parliament v Council* (EU:C:2006:346) as approved in Case C-301/06 *Ireland v Parliament* (EU:C:2009:68) and with the opinion of AG Mengozzi relating to the draft agreement between Canada and the European Union on the transfer and processing of passenger name record data (Opinion 1/15 (EU:C:2016:656), 8 September 2016). It further observed that this would also appear to be in conflict with Article 25 of the Data Protection Directive under Chapter IV of the directive, entitled "Transfer of Personal Data to Third Countries". As a result this issue now features large in the reference made by the IPT to the CJEU.

19. In these circumstances there remains considerable uncertainty in relation to this further requirement for which the Respondents and the Interveners contend. It is to be hoped that these uncertainties, which inevitably affect the vital interests of Member States, will be clarified by the CJEU when it considers the reference made by the IPT. However, as matters stand, I do not consider that this court should make a definitive statement on this issue in the form of a declaration.

Notification Requirement

20. The Respondents and the Interveners submit that this court should also make a declaration to the effect that the failure of DRIPA to make provision for ex post facto notification to persons affected infringes EU law. They base this submission on para 121 of the judgment of the CJEU which states:

> "Likewise, the competent national authorities to whom access to the retained data has been granted must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities. That notification is, in fact, necessary to enable the persons affected to exercise, inter alia, their right to a legal remedy, expressly provided for in Article 15(2) of Directive 2002/58, read together with Article 22 of Directive 95/46, where their rights have been infringed ..."

21. In my view, however, it is not appropriate to make such a declaration for the following reasons. First, this has not previously been an issue in the national proceedings. Mr Jaffey told us that this point was argued at the oral hearing of the reference in Luxembourg but he accepted that the point had only been touched on briefly in the national proceedings. Contrary to his submission, paragraph 29 of the order for reference in the present proceedings does not address this issue but the powers of the Interception of Communications Commissioner. Secondly, although the significance of this is not entirely clear, this requirement is not included in the dispositif of the CJEU judgment in the present case where the other *Watson* requirements are recited. Thirdly, it is clear that this will be an issue before

the CJEU when it considers the pending reference by the Investigatory Powers Tribunal (See IPT judgment, paragraphs 62-64).

A declaration reflecting paragraph 1 of the dispositif

22. At paragraphs 106 – 112 of its judgment the CJEU addresses the question of the relationship between the data which must be retained and a threat to public security. In this section of the judgment it is addressing the question referred by the Swedish court on the basis of the relevant Swedish legislation. At paragraph 111 the CJEU stated:

> "As regards the setting of limits on such a measure with respect to the public and the situations which may potentially be affected, the national legislation must be based on objective evidence which makes it possible to identify a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences, and to contribute in one way or another to fighting serious crime or to preventing a serious risk to public security. Such limits may be set by using a geographical criterion where the competent national authorities consider, on the basis of objective evidence, that there exists, in one or more geographical areas, a high risk of preparation for or commission of such offences."

In paragraph 112 the CJEU then states its answer to the question referred by the Swedish court in identical terms to paragraph 1 of the dispositif.

23. Mr Drabble QC, on behalf of the Second and Third Respondents, submits that this court should grant declaratory relief reflecting the fact that DRIPA does not proceed by reference to objective evidence which makes it possible to identify a public whose data is likely to reveal a link, whether direct or indirect, with serious criminal offences. On behalf of the Secretary of State, Mr Eadie submits that this passage of the judgment of the CJEU is based on the Swedish legislation and that it is not appropriate for this court to move from the general principle stated by the CJEU to the conclusion that DRIPA suffers from the same vice.

24. I initially took the view that the general principle stated by the CJEU at paragraphs 106-112 of its judgment and in paragraph 1 of the dispositif is one of general application and that, as DRIPA did not include any such limitations, it was appropriate to grant declaratory relief reflecting this fact. However, when a draft judgment and draft order were circulated to the parties and interveners in advance of handing down judgment, counsel for the Appellant lodged further written submissions in which they drew attention to matters which had not been drawn to our attention in the course of the oral hearing. The Appellant invited the court to decline to exercise its discretion to make the proposed declaration on this point.

25. The procedure governing the circulation of draft judgments does not permit the making of such further submissions (*R (Edwards) v. Environment Agency (Note)* [2008] 1 WLR 1587). However, it appears that there was some confusion as to the procedural steps to be taken following the oral hearing, and that the Appellant was awaiting further written submissions from the First Respondent before herself making further written submissions with the court's permission. Furthermore, in the light of the public importance of the matters raised the members of the court took the view that we should, exceptionally, invite further submissions from the Respondents and the Interveners on the matters raised by the Appellant. We have now received written submissions in response from the Respondents and the Interveners. We note, in passing, that the submissions lodged by the First Respondent do not address the current issue and those of the Second and Third Respondents simply state that the correct interpretation of paragraphs 55 to 65 of the *Digital Rights* judgment was and must have been anxiously considered by all the parties and the court during the current proceedings.

26. On further consideration, I have come to the conclusion that this court should decline to grant declaratory relief under this head for the following reasons.

(1) First, I am satisfied that this specific point has not been in issue in the present proceedings. In particular, it has not previously been argued in these proceedings that DRIPA was unlawful because it did not require there to be an identified public whose data was likely to reveal a direct or indirect link with serious criminal offences. There has been no evidence or argument on this point specific to DRIPA. The issue has been raised for the first time only following the decision of the CJEU in relation to the Swedish legislation. On the contrary, it has been the position of the Respondents that EU law permits a general retention regime provided it is accompanied by appropriate safeguards for access. During the course of argument before the Divisional Court, counsel for the First Respondent accepted that the CJEU in *Digital Rights Ireland* "cannot have meant that [communications service providers] can only lawfully be required to retain the communications data of "suspects or persons whose data would contribute to the prevention, detection or prosecution of serious criminal offences" as such a restriction would be wholly impracticable (Divisional Court Judgment at paragraph 70). Before this court the Respondents expressly adopted the conclusion of the Divisional Court that "the solution to the conundrum" is that "a general retention regime for communications data infringes ... the EU Charter unless it is accompanied by an access regime (laid down at national level) which provides adequate safeguards for those rights." (Divisional Court Judgment, at paragraph 89; First Respondent's Skeleton Argument, at paragraph 59; Second and Third Respondents' Skeleton Argument at paragraph 8).

(2) Secondly, the reasoning of the CJEU at paragraphs 106 – 112 is closely linked to the language and effect of the Swedish statute and, in particular, its requirement of blanket retention of all communications data by all communications service providers. I accept that the analysis and conclusions of the CJEU in this regard are not necessarily susceptible of automatic application to the different scheme of DRIPA.

(3) Thirdly, the effect of this section of the judgment of the CJEU is a live issue in the pending proceedings in which Liberty challenges Part 4, Investigatory Powers Act 2016, which is due to be heard in February 2018. I consider that it is appropriate for this issue to be addressed in those proceedings where the court will have the benefit of detailed evidence, and full pleadings and submissions.

Terms of Declaration

27. In these circumstances I consider that it is appropriate to grant declaratory relief in the following terms:

> Section 1 of the Data Retention and Investigatory Powers Act 2014 was inconsistent with EU law to the extent that, for the purposes of the prevention, investigation, detection and prosecution of criminal offences, it permitted access to retained data:-
>
> (a) where the object pursued by that access was not restricted solely to fighting serious crime; or
>
> (b) where access was not subject to prior review by a court or an independent administrative authority.

Sir Geoffrey Vos, Chancellor of the High Court:

28. I agree.

Lord Justice Patten:

29. I also agree.