The Watson Case: Another Missed Opportunity for Stricto Sensu Proportionality?

Ioannis Kouvakas*

I. Introduction

On 21 DECEMBER, 2016, the Grand Chamber of the Court of Justice of the European Union (CJEU) handed down its judgment in the *Watson* case.[1] The case was brought in 2014 by Tom Watson MP and David Davies MP, from which the latter withdrew on his appointment to Government.

The judgment adds to the debate of the compatibility of mass surveillance with international and EU law, and could be considered to advance the approach adopted by the Grand Chamber of the Luxembourg Court in the *Digital Rights Ireland* case.[2] The case concerned the Data Retention Directive 2006/24,[3] which laid down the obligation for the providers of publicly available electronic communication services or of public communications networks to retain all traffic and location data "in order to ensure that the data were available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law." The Data Retention Directive was held to create a disproportionate interference with the fundamental rights enshrined in Articles 7 and 8 of the EU Charter, and was hence declared invalid.

Following the judgment in *Digital Rights Ireland*, the United Kingdom enacted the Data Retention Investigatory Powers Act 2014 (DRIPA), which sought to

* LL.B. (University of Athens), LL.M. Human Rights Law (UCL), Ioannis.kouvakas@gmail.com.

1 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 Tom Watson* [2016] ECR I–970 (Watson case).

2 Joined Cases C-293/12 and C-594-12 *Digital Rights Ireland Ltd v Minister for Communications*, *Marine and Natural Resources & Others and Seitlinger and Others* [2014] ECR I-238.

3 Directive (EC) 2006/24 of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L105/54 (Data Retention Directive).

immediately restore the powers contained in the Directive. It enabled the Secretary of State to adopt, without any prior authorisation, measures that would require public telecommunications services operators to retain all traffic and location data relating to any postal or telecommunications service for a period of up to 12 months. Watson MP and Davies MP brought a challenge against DRIPA, and the High Court of Justice (Divisional Court) held that the requirements on the retention of communications data and access to such data laid down by the CJEU in the *Digital Rights Ireland* case should be considered mandatory and applicable to the legislation of Member States. In an order dated 17 July, 2015, the Divisional Court declared section 1 of DRIPA inconsistent with EU law, mainly because the provision was identical to the ones contained in the Data Retention Directive.

The Secretary of State for the Home Department appealed against the decision of the High Court. The Court of Appeal considered that, in *Digital Rights Ireland*, the CJEU was only examining the compatibility of a Directive, and not the compatibility of national legislation with EU law, and did not therefore intend to lay down mandatory requirements that each member state should incorporate, in its domestic provisions governing retention and access to communications data. Instead, it decided to stay the proceedings and refer two questions to Luxembourg for a preliminary ruling.

The case bears significantly on the future of mass communications data retention in the United Kingdom, as well as in other member states which have enacted similar legislation. Although DRIPA has already expired, the recently minted Investigatory Powers Act 2016 (IPA) makes provision for equally—now prescribed—broad powers pertaining not only to mass communications data retention, but also to the acquisition of Bulk Personal Datasets (BPDs), and to mass equipment interference (hacking).

During the proceedings before the CJEU, *Watson* was joined with another Swedish case, brought by Tele2Sverige, a Swedish electronic communications services provider. Tele2Sverige had brought an action before the Administrative Court of Stockholm, challenging an order by the Swedish Post and Telecom Authority (PTS), by virtue of the law transposing Directive 2006/24 into Swedish legislation, to continue retaining all communications data, even after the *Digital Rights Ireland* judgment. The action had been dismissed and Tele2Sverige appealed against the decision before the Administrative Court of Appeal of Stockholm, which decided to stay the proceedings and refer to the CJEU two questions for a preliminary ruling.

II. The Judgment

The legal issues that the Grand Chamber was confronted with were, firstly, whether a general obligation to retain communications data—covering all persons, without any distinctions, for the purpose of combating crime—could be held to be compatible with Article 15(1) of Directive 2002/58/EC (Directive on privacy and electronic communications);[4] secondly, whether the Court in *Digital Rights Ireland* intended to lay down mandatory requirements of EU law that should be also applicable to a Member State's domestic legislation governing the retention and access to communications data, for it to comply with Articles 7 and 8 of the EU Charter; and, thirdly, whether the Court intended, in the aforementioned case, to expand the scope of the protection granted by Articles 7 and 8 of the Charter beyond that established by the article 8 of the European Convention on Human Rights and the relevant European Court of Human Rights (ECtHR) jurisprudence.

Regarding the first issue, the Court acknowledged that Article 15(1) of Directive 2002/58/EC allows for restrictions to the protection enshrined in the Directive—that is, the principle of confidentiality of electronic telecommunications—and does not preclude domestic legislation of Member States to introduce limitations upon the right, so long as these restrictions are necessary and proportionate, and justified by the objectives laid down exhaustively in that Article. Nevertheless, any limitation imposed upon the rights and obligations enshrined in the Directive shall be interpreted in the light of Articles 7, 8, and 52(1) of the Charter.

The Court acknowledged that the categories of data covered by national legislation correspond, in essence, to the data for which retention was required by the Data Retention Directive. Although retention did not relate to the content of communications and would not engage the essence of these rights, retention of communications data, particularly traffic and location data, allows for very precise conclusions to be drawn concerning the private lives, daily movements, permanent or temporary places of residence of persons. It also enables authorities to, inter alia, identify the names and addresses of subscribers or registered users, and should be regarded as a particularly serious and far reaching interference with the rights enshrined in the Charter. Such an interference, according to the Grand Chamber, could be justified by the objective of combatting only serious crime.

More importantly, the CJEU held that the general and indiscriminate retention of all traffic and location data was disproportionate. National legislation must lay down clear and precise rules, governing the scope and application of such a measure by ensuring that retention is limited to what is strictly necessary.

[4] Directive (EC) 2002/58 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) [2002] OJ L201/37.

Therefore, an objective link needs to exist between a public likely to be involved in serious criminal activity and the objective pursued, such as retention of data pertaining to a particular time period or geographical area or group of persons, or all three. Otherwise, the legislation fails to meet the necessity test.

Regarding the second issue, the Grand Chamber underlined that, irrespective of a general or targeted retention of communications data, domestic legislation must make provision for adequate safeguards, which would either provide sufficient guarantees against abuse, or counterbalance risk of abuse. Three minimum safeguards were held to be mandatory. First, access should be granted to the data of individuals suspected of planning, committing or having committed a serious crime or having or being implicated in such nefarious criminal activity. Second, with the exception of urgent cases, such access should be granted only subject to prior review by a court or an independent administrative body following a request made by the competent authorities. Finally, traffic and location data must be retained within the EU.

The judgment also refers to the obligation of national authorities to notify the persons to whose communications data access has been granted, as soon as such a notification is practically possible without the risk of jeopardising an ongoing investigation. In this manner, these persons will be able to fully exercise their right to a legal remedy and challenge these measures successfully, in the event that their rights are infringed.

Regarding the third issue, stemming from the second question referred by the English Court of Appeal, the CJEU reiterated that while Article 52(3) is intended to ensure the necessary consistency between the Charter and the ECHR, it does not prevent EU law from providing more extensive protection than the ECHR. Further, Article 8 of the Charter constitutes a fundamental right different from that enshrined in Article 7, a right which has no equivalent in the ECHR. Nevertheless, the Court declared the question inadmissible, because it did not appear that an answer to it would provide an interpretation of EU law necessary for the English court's ruling in light of the *Watson* case.

III. Comment

The reasoning of the Grand Chamber in *Watson* signals a hardened stance by the Court to accept mass surveillance measures without the existence of stringent safeguards, and especially prior review by an independent judicial or administrative body. It also raises some interesting issues concerning the application of the principle of proportionality in the context of general surveillance measures. Although the Strasbourg Court also engages in a similar assessment under the

ECHR when it comes to qualified rights, the proportionality test applied by the CJEU is a more structured one, and is quite similar to the one applied by English courts in the context of human rights adjudication. Actually, in determining whether an interference with a right shall be deemed proportionate, the principle of proportionality could be further formulated into (two) separate stages: necessity and *stricto sensu* proportionality.

Necessity, in the human rights context, is interpreted as the requirement of "less restrictive means", meaning that when another means exists that could achieve the same result with less onerous implications, the more human rights compliant alternative must be chosen. A necessity assessment does not imply, of course, that an interference with the right must always be minimal.[5] What is important for the necessity stage is the measure to be precisely tailored to its aim. On the other hand, certain policies which affect more individuals than necessary could be characterised as over inclusive or, in certain cases, indiscriminate.

What the Grand Chamber ruled in both *Watson* and *Digital Rights Ireland* was that indiscriminate data retention measures are, in principle, disproportionate. They fail to satisfy the necessity test because of their indiscriminate nature. In other words, the CJEU held that a general measure to retain the traffic and location data of all individuals, without differentiation, cannot be precisely tailored to the aims pursued by the legislative objective and thus, in principle, contradicts necessity. In that regard, the reasoning of the Court remains unsatisfactory mainly for two reasons.

First, retention of traffic and location data is, by its very nature, an indiscriminate measure. It cannot target specific individuals, unlike targeted interception warrants, because its purpose is to identify potential threats and provide important information for persons that might in the long term prove to engage or to have engaged in nefarious activities. Therefore, the basic characteristic of communications data retention, and of bulk surveillance in general, is the lack of "reasonable suspicion", which otherwise serves as an effective safeguard, strengthening the foreseeability of the law and preventing the risk of discriminatory abuses on a subjective basis. Thus, the question to be addressed is whether the indiscriminate (strategic) retention of communications data can incorporate a reasonable suspicion criterion, and still fulfil the aim of effectively identifying potential or future threats.

The CJEU attempted to answer this question in the affirmative by inserting some "objective criteria" that would render the data retention less indiscriminate, namely criteria pertaining to a certain time period, geographical area or group of

[5] Aharon Barak, Proportionality*: Constitutional Rights and their Limitations* (Cambridge University Press 2011) 321.

persons for a link to be established between persons who are likely to have engaged in serious crime and the aim pursued. In the context of contemporary pre-empting technologies, however, the application of a reasonable suspicion standard remains problematic.

It is worth noting here that a similar approach was adopted by the ECtHR in the case of *Marper v UK*.[6] The reasoning of the Strasbourg Court was extensively followed by the Grand Chamber in *Digital Rights Ireland*. In *Marper*, the ECtHR was confronted with the legal issue of whether an Act providing for the indefinite retention of fingerprints, as well as cellular and DNA samples taken by anyone accused of an offence irrespective of their consequent conviction or acquittal, could be held to be proportionate, and, in particular, to successfully pass the necessity test under Article 8 of the Convention. The Strasbourg Court held that a blanket DNA retention policy fails to satisfy the necessity stage and is thus, in principle, a disproportionate interference with the right to private life.[7]

However, this reasoning is flawed because the ECtHR, instead of addressing the moral question of whether the retention of cellular samples and DNA profiles was justified under the Convention, stopped at the necessity stage of its overall proportionality assessment.[8] It ruled that blanket policies are, in principle, incompatible with Article 8, and stressed that a differentiation should be made between convicted and unconvicted individuals, giving the impression that unconvinced persons have more of a *pro tanto* right to privacy than convicted persons. The implications of *Marper* on a domestic level are obvious if one looks at the case of *Gaughran*.[9] In that case, the Supreme Court held that the measure of indiscriminate retention of DNA profiles, fingerprints and photographs of all adults convicted of recordable offences was compatible with Article 8 of the ECHR. Interpreting *Marper* by the same token, the Supreme Court found that "[T]here is no indication that the Strasbourg court was considering the position of those who had been convicted at all … Strasbourg was not saying that a blanket policy of [indefinitely] retaining the data of convicted persons would be unlawful".[10]

In the case of *Szabo and Vissy*, the ECtHR appeared to gradually abandon the reasonable suspicion requirement, placing greater emphasis on the importance

6 *S and Marper v UK* (2008) 48 EHRR 50.

7 ibid, para 125.

8 George Letsas, 'The scope and balancing of rights: Diagnostic or constitutive?' in Eva Brems and Janneke Gerards (eds), *Shaping Rights: The Role of the European Court of Human Rights in Determining the Scope of Human Rights* (Cambridge University Press 2015) 59.

9 *Gaughran v Chief Constable of the Police Service of Northern Ireland* [2015] UKSC 29. For an overview and assessment of the current DNA (and, generally, biometrics) retention regime, see Paul Wiles, '2016 Annual Report of the Commissioner for the Retention and Use of Biometric Material' (September 2017).

10 ibid *Gaughran* [31]–[33].

of other safeguards, especially prior judicial authorisation.[11] In his Opinion in the *Watson* case, the Advocate General concluded that bulk surveillance is not in principle unlawful if it is accompanied by all safeguards considered by the CJEU in *Digital Rights Ireland*.[12] Reasonable suspicion, however, was one of the main safeguards that the Court noted the Directive had failed to incorporate. In other words, the Advocate General argued that the reasonable suspicion criterion could still be excluded, as long as bulk surveillance satisfies the requirements of strictly defined purposes, prior independent (judicial) authorisation and minimum retention periods to what is strictly necessary.[13] In that regard, the Grand Chamber was right in holding that the requirements laid down in *Digital Rights Ireland* should be considered mandatory.

Second, limiting retention to certain time periods, geographical areas, or groups of persons ultimately reduces the efficiency of the measure.[14] Hence, the existence of a less injurious alternative does not necessarily imply that this alternative has to be chosen if it is less effective in advancing the means pursued by the choices of the legislature.[15] This view was endorsed by the Canadian Supreme Court in the case of *USA v Cotroni*,[16] which concerned an extradition law according to which Canadian citizens could also be extradited. The Supreme Court examined the indiscriminate nature of the law, noting that "the effective prosecution and the suppression of crime is a social objective of a pressing and substantial nature", and held that an alternative policy of refusing to extradite Canadian citizens "would reduce the effectiveness of extradition as a major tool in combatting transnational crime".[17]

In examining the question of whether a general data retention obligation is proportionate, contrary to the submissions of Tele2Sverige, Privacy International and Open Rights Group that any general (blanket) data retention obligation should be *per se* regarded as violating the principle of necessity, because of their inherently

[11] *Szabo and Vissy v Hungary* App no 37138/14 (ECtHR, 12 January 2016), paras 68 and 73.

[12] Opinion of Advocate General Saugmandsgaard Øe 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 Tom Watson* [2016] ECR I–572, para 202 (Watson AG Opinion).

[13] ibid, para 244.

[14] T. Raine, 'The CJEU and Data Retention: A Critical Take on the Watson Case', (UK Const. L. Blog, 16 January 2017) <https://ukconstitutionallaw.org/2017/01/16/thomas-raine-the-cjeu-and-data-retention-a-critical-take-on-the-watson-case> accessed 20 September 2017.

[15] Tom Hickman, *Public Law after the Human Rights Act* (Hart 2010) 181; Barak (n 6) 323.

[16] *USA v Cotroni* [1989] 1 S.C.R. 1469.

[17] ibid, 1499; *USA v. Swystun* (1987) 50 Man. R. (2d) 129, 133. See also HCJ 7052/03 *Adalah–The Legal Center for the Rights of the Arab Minority v Minister of Interior* (unpublished, 14 May 2006), para 88.

over-inclusive character,[18] the Advocate General stated that the obligation did not go beyond what was strictly necessary, but it was because of the "combined effect of the generalised retention of data and the lack of safeguards aimed at limiting the interference with the rights enshrined in Articles 7 and 8 of the Charter"[19] to what was strictly necessary that led the Luxembourg Court to declare the Directive invalid in its entirety. He then stated:

[T]he requirement of strict necessity … requires a comparison to be made between the effectiveness of such an obligation and that of any other possible national measure ... Nevertheless, it is important to bear in mind that any substantial limitation of the scope of a general data retention obligation may considerably reduce the utility of such a regime in the fight against serious crime.[20]

According to the Advocate-General, the issue of proportionality of such measures had thus to be determined at the final *stricto sensu* stage by national courts, which are called to weigh the advantages of such techniques and the serious risks that arise from such intrusive powers. The Advocate General then referred to the policy of installing a GPS tracking device on each and every citizen for the purposes of combatting crime; an indiscriminate measure that would, for the reasons illustrated above, satisfy necessity considerations. This does not necessarily imply that the measure would still be *stricto sensu* proportionate since, in this case, the aim sought to be achieved does not outweigh the overall impact on the individuals' rights.[21]

A similar question arises in relation to a blanket obligation imposed upon telecommunications service providers to retain traffic and location data. Considering the particularly manifold and serious interference with the fundamental right to privacy, the question that needs to be addressed is whether national authorities can strike a fair balance between competing public interests, such as the fight against serious crime, and fundamental rights of persons enshrined in Articles 7 and 8 of the Charter.[22]

[18] Watson AG Opinion (n 12), para 192.

[19] ibid, para 202; C362/14 *Schrems v Data Protection Commissioner* (CJEU, 6 October 2015), para 93.

[20] ibid Watson AG Opinion (n 12), paras 207 and 213. As regards the importance of bulk powers for safeguarding national security, see David Anderson, 'Report of the Bulk Powers Review' (2016) paras 6.47 and 9.14(b) <https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf> accessed 20 September 2017; Privacy International v Secretary of State for Foreign and Commonwealth Affairs [2017] UKIPTrib IPT_15_110_CH paras 14–17; European Commission, 'Evaluation Report on the Data Retention Directive (Directive 2006/24/EC)' COM (2011) 225 final 25.

[21] ibid Watson AG Opinion (n 12), paras 261-262.

[22] David Anderson, 'CJEU Judgment in Watson' (21 December 2016) <https://terrorismlegislationreviewer.independent.gov.uk/cjeu-judgment-in-watson> accessed 20 September 2017.

IV. Conclusion

In sum, the judgment of the Grand Chamber in *Watson* should be welcomed as an advance towards more robust safeguards in the context of bulk interception powers. The CJEU seems to embrace the argument that, because of its peculiar characteristics, mass surveillance cannot be treated the same as targeted interception techniques. Nevertheless, this flexible approach towards mass surveillance should not be interpreted as an effort to circumvent stringent controls but as an effort of the Court to adapt to cutting edge pre-empting technologies.

By ruling, however, that indiscriminate communications data retention policies in principle contradict necessity and by focusing on such quantifiable aspects of a case, the Court seems to withdraw "from a battle regarding the general principle without a fight".[23] In other words, in an ultimate attempt to limit the scope of a generalised data retention obligation, the Grand Chamber inserted criteria, such as that of particular time periods or geographical areas, which could establish an objective link between potential threats and the aim pursued.

All in all, the judgment still strikes a massive blow to indiscriminate communications data retention measures *per se* and, although DRIPA expired at the end of December 2016, raises compatibility issues with the data retention principles set out by the European Court regarding bulk powers contained in the recently passed IPA.[24]

More specifically, IPA provides, among others, for the obtaining and retention of metadata in bulk,[25] as well as for bulk personal datasets (BPDs) acquisition[26] and equipment interference (hacking).[27] As regards the former, the current IPA authorisation regime allows for access to retained communications data to be

[23] Stavros Tsakyrakis, 'Proportionality: An assault on human rights?' (2009) 7 IJCL 486.

[24] Cf *Privacy International* (n 21), concerning the lawfulness of the Security and Intelligence Services' capability to acquire and use communications data, pursuant to s. 94 of the Telecommunications Act 1984 (which requires communications data to be delivered up to security and intelligence services so as to constitute bulk communications data in their custody, access to which could be later granted either for targeted purposes or for, more likely, the electronic trawling of masses of data in order to discover "the needle in the haystack"), and personal datasets in bulk. In October 2016, the Investigatory Powers Tribunal ruled that, albeit lawful in domestic law, those regimes had not been ECHR compliant prior to their public avowal, see *Privacy International v Secretary of State for Foreign and Commonwealth Affairs* [2016] HRLR 21. However, while acknowledging that a similar application of the Watson requirements to the regime governing the bulk acquisition of communications data by the security and intelligence services may seriously impede national security capabilities of the services, the IPT eventually decided to refer the issue of compatibility of s. 94 with EU law to the CJEU, see *Privacy International* (n 21) paras 69 and 72.

[25] Investigatory Powers Act 2016, pts 3 and 4.

[26] ibid, pt 7.

[27] ibid, pt 6.

granted on the basis of internally signed off warrants by senior officers within the public authority requesting access,[28] It also allows for access to be granted "for the purpose of preventing or detecting crime or of preventing disorder",[29] namely any crime and not just serious one. To adhere to the safeguards upheld by the Luxembourg Court, a legislative amendment of these provisions is required that limits the purpose of access to metadata to serious crime only, and ensures that access warrants are *ex ante* reviewed and approved by an independent authorising body, such as the one already provided for in the Act (Judicial Commissioners). However, the long-term consequences of the judgment in light of an imminent Brexit, which might well hinder any external pushes coming from the European Court,[30] remain to be seen with the assistance of the Court of Appeal to which the answers have now been returned.

[28] ibid, s 61(1) and (2), although prior judicial authorisation to access data is required for local authorities.

[29] ibid, ss 87 and 61(7)(b). Section 67(1) includes purposes far wider than serious crime such as taxation, the functioning of financial markets, and national security. For the lack of statutory definition and wide judicial interpretation of the latter see *R (Lord Carlile) v SSHD* [2014] UKSC 60.

[30] Bingham Centre for the Rule of Law, APPG on the Rule of Law, 'EU Law, the Investigatory Powers Act, and UK-EU Cross-Border Crime and Security Cooperation' (14 March 2017) 4. <https://www.biicl.org/documents/1634_2017-04-29_-_appg_report_14_march_2017.pdf?-showdocument=1> accessed 20 September 2017.