THE INTERPRETATION OF THE CHARTER OF FUNDAMENTAL RIGHTS OF THE EU IN DATA RETENTION CASES: NATIONAL IMPLEMENTATION AND POSSIBLE CHANGES OF POLICY*

TOMÁŠ OCHODEK

Abstract:

The Court of Justice of the EU has, on several occasions, ruled on the compatibility of so-called data retention measures with the Charter of Fundamental Rights of the EU. In particular, it has ruled that general and indiscriminate retention of certain electronic communications data is incompatible with Articles 7 and 8 of the Charter, be it in the form of EU secondary law or national legislation. Many Member States, however, still keep in place data retention measures contrary to these rulings, and progress in implementing the rulings is slow. At the same time, the rulings of the Court of Justice can also be interpreted as requiring a fundamental change in how these measures are used and how effective they can be.

Keywords: Charter of Fundamental Rights of the EU; data retention; national implementation; data protection

Klíčová slova: Listina základních práv EU; uchovávání údajů; vnitrostátní implementace; ochrana osobních údajů

DOI: 10.14712/23366478.2018.41

1. INTRODUCTION

In a series of cases starting with the *Digital Rights Ireland* judgement, the Court of Justice of the EU (Court, Court of Justice, or CJEU) has reviewed a number of regimes within the scope of EU law regulating mass retention of data. These cases led to the invalidation of the Data Retention Directive and a finding of incompatibility of national data retention regimes which enable the bulk collection of data.

Firstly, this article presents the key points of the Court's findings. Secondly, it looks at the impact of the Charter of Fundamental Rights of the EU (Charter) (through the Court's interpretation) on Member States with regard to their obligations to implement the rulings. Finally, this article seeks to place the data retention cases into a wider policy context – i.e. the use of big data analytics in law enforcement and the necessity of

* The paper was supported by the Charles University grant, Specific University Research ("SVV") project 2017–2019, No. 260 361.

practices such as data retention on a scale as formerly required by the Data Retention Directive.

2. DATA RETENTION: THE DIRECTIVE AND THE CASES

Under the E-Privacy Directive,[1] Member States were allowed to adopt data retention rules to safeguard the objectives listed pursuant to the limitations contained in its Art. 15 (1). The Data Retention Directive[2] was (according to its recitals) adopted in 2006 as a result of the differences between these regimes.[3] The possibility given to Member States by Art. 15 (1) of the E-Privacy Directive was thus curtailed to the extent that the Data Retention Directive harmonised the rules.

The core of the Directive was an obligation placed on providers of publicly available electronic communications services or public communications networks to retain certain data generated or processed by them while providing communication services for a period of up to two years.[4] Such data could then be accessed and used by national authorities. Additionally, in Art. 7 the Directive placed minimum requirements to be imposed on the above-mentioned providers.

The Directive was based on Article 95 EC (Art. 114 TFEU) as an internal market harmonisation of conditions for conducting business for providers of electronic communications, notwithstanding the fact that a large part of the reasoning in favour of data retention as a practice came from findings not concerned with the internal market in itself.[5] Accordingly, in *Ireland v. Parliament and Council*,[6] the Court of Justice examined the Directive in light of its case law on the correct choice of legal basis and rejected Ireland's claim.[7] While the Directive sustained this challenge, it was later proposed that the very reasons why it had been compatible with the internal market legal basis put it at odds with provisions on fundamental rights in the Charter.[8] Over time, a number of the

---

1 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), OJ L 201, 31. 7. 2002, p. 37.

2 Directive 2006/24/EC 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, OJ L 105, 13. 4. 2006, pp. 54–63.

3 Data Retention Directive, recitals 4–6.

4 See in particular Arts. 1(1) and (2), 2(2)(a), 3(1) and 6 of the Directive.

5 See in particular the importance of data retention as a valuable tool for the fight against crime coming from the Justice and Home Affairs and the Council Declaration on Combating Terrorism in recitals 7–10, stating e.g. that *'*[…] *retention of data has proved to be* […] *a necessary and effective investigative tool for law enforcement in several Member States, and in particular concerning serious matters such as organised crime and terrorism* […]*'* which will be further examined in the third part of this article.

6 Case C-301/06 *Ireland v. European Parliament and Council of the European Union*, ECLI:EU:C:2009:68.

7 Ireland, who favoured adoption of a framework decision instead of an internal market directive, unsuccessfully argued that the Directive in fact pursued the sole aim of prosecution of crime or that even if the Court found a dual purpose in the Directive, the predominant one rested in crime prosecution. See paras 28-31 and 91 of *Ireland v Parliament and Council*.

8 See Opinion of AG Cruz Villalón in the Case C-293/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, ECLI:EU:C:2013:845, para 102: *'In summary, Directive 2006/24 would fail the proportionality test for*

highest courts in EU Member States examined the legality of national implementation rules[9] and the question of the Directive's validity found its way to the Court of Justice in the *Digital Rights Ireland*[10] case through Irish and Austrian courts and in the process gave the Court the opportunity to give interpretation on both Article 7 and Article 8 of the Charter.

The Grand Chamber judgement started with one of the referred questions (which, given the results of the proceedings, was eventually the only point necessary to examine) noting that: *'*[…] *the referring courts are essentially asking the Court to examine the validity of [Data Retention Directive] in the light of Articles 7, 8 and 11 of the Charter.'*[11] Both the Advocate General and the Grand Chamber agreed that the data retention obligation laid down by the Directive created a 'particularly serious' interference with fundamental rights under Arts. 7 and 8 of the Charter. As the Advocate General (AG) noted, there was no point in arguing whether the Directive constituted an 'interference' with the right to privacy,[12] however, in light of the particular context, it was necessary to inquire whether such interference was not even more worrying.[13]

Even though the content of communication was not covered by the retention obligation, the collection and retention of personal data relating to the everyday communications of Union citizens according to the AG constituted a *'*[…] *serious interference with [their] privacy* […]*'* and a *'permanent threat throughout the data retention period'* to

---

the very reasons which justified its legal basis. The reasons for its legitimacy in terms of its legal basis would, paradoxically, be the reasons for its illegitimacy in terms of proportionality.' See also GALLI, F.: Digital Rights Ireland as an Opportunity to Foster a Desirable Approximation of Data Retention Provisions. *Maastricht Journal of European and Comparative Law*, 2016, No. 3, pp. 464 and 466.

9 Including the Judgement of the Czech Constitutional Court of 22 March 2011 *Pl.ÚS 24/10,* in which, however, the court refrained from referring to the Court of Justice for a preliminary ruling on the question of validity of the Directive, despite the fact that the concern was mentioned in the decision (see para 55); according to the Constitutional Court, the Directive did leave sufficient space for the national legislature to implement it in a legally conforming way into the national legal order (see para 25). See also MOLEK, P.: Czech Constitutional Court Unconstitutionality of the Czech Implementation of the Data Retention Directive; Decision of 22 March 2011, Pl. ÚS 24/10. *European Constitutional Law Review,* 2012, No. 2, p. 338. The legal changes necessitated by the judgement and the compatibility of the current framework are analysed in the second part of this article.

10 Case C-293/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, ECLI:EU:C:2014:238.

11 I.e. the compatibility with the respect for private life and communications under Article 7 of the Charter, the protection of personal data under Article 8 of the Charter and respect for freedom of expression under Article 11, limiting itself however, to the assessment of the compatibility with the first two Articles. See *Digital Rights Ireland*, para 23. See also on the (combined) use of Article 7 and 8 and their distinction LYNSKEY, O.: Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order. *International & Comparative Law Quarterly,* 2014, No. 3, p. 569–597 and paras 55–67 of the Opinion.

12 Note that the use of the right to privacy instead of referring to both rights under Arts. 7 and 8 of the Charter here is merely reproducing the AG's approach, which follows from his analysis concluded in para 67 of his Opinion.

13 The AG bases this on the wording of the Directive itself in recital 9, as well as on the case law of the European Court of Human Rights (see the reference in para 60 on the notion that regardless of whether the data was used, the storage of personal data by a public authority constitutes an interference with fundamental rights; see para 33 of the judgement for a connected reasoning, with the use of Joined Cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk and Others,* ECLI:EU:C:2003:294 as the basis for this claim).

such right.[14] The Opinion also stressed the impact of the everyday use of digital mobile networks and Internet.[15] Thus, in spite of the particular character of communications data, the use of such retained data could *'*[…] *make it possible to create a both faithful and exhaustive map of a large portion of a person's conduct strictly forming part of his private life, or even a complete and accurate picture of his private identity.'*[16]

The Grand Chamber subscribed to the concerns of the AG regarding the possibility to derive such information form retained data.[17] Indeed, the judgement similarly stated that *'*[*such*] *data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.'*[18]

The Court found that there was no intrusion into the essence of either Art. 7 or Art. 8 of the Charter[19] and that the Directive satisfied an objective of general interest.[20] In the assessment of appropriateness of the regime for the fight of serious crime, the judgement quickly found that while there were possibilities which enable to circumvent the data retention regime and provide anonymised communication, the Directive was nonetheless appropriate to achieve its aim; the Court noted that the Directive *'*[*allowed*] *the national authorities which are competent for criminal prosecutions to have additional opportunities to shed light on serious crime and, in this respect,* [*was*] *therefore a valuable tool for criminal investigations* […]*.'*[21]

The key part of the judgement relates to the necessity of the data retention regime vis-à-vis the legitimate objective; the Court noted that while: *'*[…] *the fight against serious crime, in particular against organised crime and terrorism, is indeed of the utmost importance in order to ensure public security and its effectiveness may depend to a great extent on the use of modern investigation techniques* […]*'*that alone could not justify the interference caused by the Directive. Inspired by the case law of the European Court of Human Rights,[22] the judgement stated that: *'*[…] *EU legislation in question must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards* […] *against the risk of abuse and against any unlawful access and use of that data*[.]*'* Two sets of objections present in the reasoning are summarised below.

Firstly, the Court strongly objected to the very broad scope of the retained data – all communications data pursuant to the Directive were to be retained without any differen-

---

14 *Digital Rights Ireland Opinion*, para 72.
15 *Digital Rights Ireland Opinion*, paras 73–75.
16 *Digital Rights Ireland Opinion*, para 73; see also *Digital Rights Ireland Opinion*, para 72 and *Digital Rights Ireland*, para 37.
17 *Digital Rights Ireland*, paras 32–37.
18 See *Digital Rights Ireland*, para 27; even though this paragraph actually preceded the relevant part of the analysis in the judgement, it relates essentially to the same point of concern.
19 *Digital Rights Ireland*, paras 39–40.
20 *Digital Rights Ireland,* para 42.
21 *Digital Rights Ireland,* para 49; more on the findings of the Court of Justice as well as corresponding concerns about the suitability of data retention are dealt with further in the second part of this article.
22 See references in para 54 of *Digital Rights Ireland.*

tiation, limitation, or exception[23] and covering (and interfering with the fundamental rights of) practically the entire European population.[24] A person's communication data could be collected and retained irrespective of whether that person had any link to the perpetration of serious crime; more precisely, there was no requirement for the data in question to have a relationship to either certain geographical area, time, circle of persons, or persons who could otherwise contribute to the investigation of serious crime.[25]

Secondly, further objections related to, broadly described, the more practical aspects of the data retention regime. For example, concerning the retained data, the Directive did not contain *'*[…] *substantive and procedural conditions relating to the access* […] *and their subsequent use* […]*'* and did not expressly limit such access and use to what would be strictly necessary;[26] similarly, no limitation of the number of persons with such access was present.[27] In a similar reasoning, the Court found the lack of criteria for determination of an actual retention period unsatisfactory (with the 6–24 months provision being too vague).[28] Subsequently, the Court also took issue with the conditions under which data was to be retained by the communication service providers, citing the lack of rules designed to respond to the quantity and sensitive nature of such data, as well as the lack of provisions preventing unlawful access and use,[29] with no sufficient guarantees that data would be irreversibly destroyed upon the lapse of retention period or that such data would be kept within the EU.[30]

Consequently, the Court held that the Directive *'*[*did*] *not lay down clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter* […]*'* and that the particularly serious interference (see above) was not *'*[…] *precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary* […]*'*[31] and declared the Directive as a whole invalid.

The approach of the Court in *Digital Rights Ireland* was subsequently confirmed on two occasions by the Court: in *Tele2/Watson*[32] and *Opinion 1/15*.[33]

Tele2/Watson dealt with the issue of the legality of national data retention measures (originally implementing the now invalid Directive); the Court clarified two points already touched upon in the *Digital Rights Ireland* judgement.[34] Firstly, in interpreting

---

23 Highlighting in particular the communications normally protected by professional secrecy; see para 58.
24 *Digital Rights Ireland,* paras 56–57.
25 *Digital Rights Ireland*, paras 58–59; additionally, the Court expressed objections to the fact that the notion of 'serious crime' was to be defined according to national law in para 60.
26 *Digital Rights Ireland*, para 61.
27 *Digital Rights Ireland*, para 62.
28 *Digital Rights Ireland*, paras 63–64.
29 *Digital Rights Ireland*, para 66.
30 *Digital Rights Ireland*, paras 67–68; see also paras 75–77 of the Opinion.
31 *Digital Rights Ireland*, para 64; See for reaction to the case: LYNSKEY, O.: The Data Retention Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety: Digital Rights Ireland. *Common Market Law Review*, 2014, No. 6, p. 1789–1812.
32 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 and Others***,** ECLI:EU:C:2016:970.
33 *Opinion 1/15*, ECLI:EU:C:2017:592.
34 See also clarifications on the scope of Art. 15 (1) of the E-Privacy Directive in paras 64–81, and the elements falling within that scope in paras 72, 77, and 79 of the judgement.

Art. 15 (1) of E-Privacy Directive in light of Arts. 7, 8, 11, and 52 (1) of the Charter, the Court clarified that the obligation to collect and retain communications data may only be justified by the objective of fighting *serious* crime.[35] It also found that the national legislation laid down the data retention obligation essentially similar to the invalid Data Retention Directive.[36] It then held that even an objective such as the fight against organised crime or terrorism *'*[…] *however fundamental it may be, cannot in itself justify that national legislation providing for the general and indiscriminate retention of all traffic and location data should be considered to be necessary for the purposes of that fight*[.]*'*[37] Instead, the Court stated, not precluding data retention altogether, that a targeted form of retention would not run into these objections (this notion will be further examined in the second part of this article).[38] On the second point, the Court confirmed its approach regarding the practical aspects relating to data retention and restated some key points which the national legislation must comply with.[39] Eventually, the Court found that both national implementations were in breach of Art. 15 (1) of E-Privacy Directive as interpreted in the case.

This line of reasoning was then again *broadly* (see part three of this article) confirmed in the *Opinion 1/15* which concerned the legality of a negotiated agreement on the exchange of PNR (Passenger Name Record – set of data on passengers on EU-Canada flights) data.[40]

3. IMPLEMENTATION OF *DIGITAL RIGHTS IRELAND* AND *TELE2/WATSON* BY MEMBER STATES

The *Digital Rights Ireland* case was suggested to be an opportunity to reformulate the European data retention framework in a way that would remedy certain issues that were not properly resolved during the adoption of the Data Retention Directive as well as to reframe the directive (or regulation if that were to be the way forward) to make it compliant with fundamental rights under the Charter.[41] Instead, no act has been adopted to replace the invalid directive so far.

The two judgements analysed above related to the interpretation of the framework laid down by the E-Privacy Directive; as a part of a privacy and data protection legislation overhaul, the E-Privacy Directive is to be replaced by a Regulation carrying the

---

35 *Tele2/Watson,* para 102; this clarified the wording of the E-Privacy Directive, which in its relevant part of Art. 15 (1) states that limitation on fundamental rights in the form of data retention may be adopted inter alia for the purpose of *'prevention, investigation, detection and prosecution of criminal offences'*.

36 *Tele2/Watson,* para 97.

37 *Tele2/Watson,* para 103; compare to the Opinion of Advocate General Saugmandsgaard Øe in the 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 and Others,* ECLI:EU:C:2016:572.

38 *Tele2/Watson,* paras 108 and 110.

39 *Tele2/Watson,* paras 115–123; for instance, save for exceptional situations, access should be only granted to data concerning persons implicated at least to a certain degree in criminal activity; see, however, para 115.

40 *Opinion 1/15*, paras 163 and 202.

41 Galli (see note 8), pp. 466–469 and pp. 470–472 respectively.

same (short) name – E-Privacy Regulation. The Regulation, according to the Commission proposal,[42] does not contain any specific provisions on data retention.[43] Instead, it works with a scheme similar to the one presented by Art. 15 (1) of the E-Privacy Directive: Member States are free to adopt (and keep, where those already exist) data retention measures as restrictions on scope of rights and obligations in the Regulation under its Article 11; the objectives pursued by such (legislative) measures are not expressly named in the E-Privacy Regulation, but must correspond to grounds enumerated in Art. 23 (1) a) to e) of the General Data Protection Regulation.[44] Furthermore, references are specifically made to the two judgements and the 'targeted' nature (which will be explained below) of any permissible data retention measure.[45]

The rate of implementation of the judgements has been subjected to considerable criticism, especially from privacy-oriented NGOs.[46] The latest annual report of the EU Fundamental Rights Agency similarly states that the progress of national lawmakers has been rather limited, noting that Member States seem to be reluctant to change the existing frameworks.[47]

The progress so far can be illustrated as follows. On the issue of conditions of access, delineation of crimes the prosecution of which enables the use of the retained data, storage within the EU and similar conditions relating to the practical operation of the system, several Member States are taking up the task given to them by the Court's rulings and are remedying (or already have done so) the shortcomings in their national

---

42 Commission Proposal of 10 January 2017: Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications); available from: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241 [accessed 8 May 2018], see p. 3 of the proposal.

43 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4 May 2016, pp. 1–88); It should also be emphasised that the Commission proposal is obviously only a starting point in the legislative process and changes not only may be made, but at the time of the writing of this article (and in the latest proposal known to the author), the Bulgarian Presidency of the Council already suggested some changes to the regime in the proposal of 4 May 2018: Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), available from: http://data.consilium.europa.eu/doc/document/ST-8537-2018-INIT/en/pdf [accessed 8 May 2018].

44 See Commission Proposal (note 42); See however p. 6 of the Bulgarian Presidency Proposal (note 43).

45 See Commission Proposal (note 42), p. 3.

46 See for instance: Member State data retention regimes – what's changed? The answer is very little so far. In: *Statewatch* [online]. 2017 [accessed 8 May 2018]. Available from: http://www.statewatch.org/news/2017/nov/eu-eurojust-datret-regimes.htm or: EU Member States plan to ignore EU Court data retention rulings. In: EDRi [online]. 2017 [accessed 8 May 2018]. Available from: https://edri.org/eu-member-states-plan-to-ignore-eu-court-data-retention-rulings/.

47 European Union Agency for Fundamental Rights. *Fundamental Rights Report 2017* [online]. Publications Office of the European Union, 2017 [accessed 10 May 2018]. Available from: http://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-fundamental-rights-report-2017_en.pdf, p. 163; Note also that in some of the most recent developments, the actual implementation of the judgements seems to be in question: WHITE, M.: Data Retention incompatible with EU law: Victory? Victory you say? In: *EU Law Analysis Blog* [online] 2018 [accessed 22 August 2018] Available from: http://eulawanalysis.blogspot.com/2018/05/data-retention-incompatible-with-eu-law.html.

legislation.[48] Several Member States, Slovakia included, have already repealed or reformed their data retention frameworks altogether.[49]

On the other hand, for a large number of Member States, the remaining issue is the scope of the data retention obligations still present in national law as bulk data retention remains in place in many countries.[50] In *Tele2/Watson*, while refusing to condone general and indiscriminate data retention (see above), the Court has also ruled that the E-Privacy Directive read in light of the Charter of Fundamental Rights of the EU *'[…] does not prevent a Member State from adopting legislation permitting, as a preventive measure, the targeted retention of traffic and location data, for the purpose of fighting serious crime, provided that the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary.'*[51] Nonetheless, according to Eurojust, no Member State is currently close to achieving this model – while Germany reported an exclusion of a certain category of data relating to the church, that does not (while reducing the scope of data a little bit) remove the characteristic of a national data retention framework as a general one.[52]

The current form of the Czech legislation resulted from a reaction to the invalidation of the original data retention provisions in the Electronic Communications Act by the Czech Constitutional Court even prior to the *Digital Rights Ireland* judgement. Parts of the original Art. 97 of Electronic Communications Act were struck down due to a number of shortcomings, including the lack of a sufficiently detailed description of authorities that could access the data,[53] the lack of a precisely delineated purpose for enabling access (where the national legislation did not limit access to the fight against *serious* crime),[54] the lack of notification of individuals,[55] or little to no provisions on security safeguards.[56] On the contrary, the bulk nature of collection and retention of data in itself was not taken as a reason to invalidate the provisions.[57]

---

48 FRA Report (note 47), p. 165.

49 See FRA Report (note 47), p. 164 with reference to the Slovak Act No. 397/2015 Coll. from 13 November 2015, which for the purposes of the Criminal Code provides a list of substances with anabolic or other hormonal action and amending and supplementing certain laws; see also Data retention regimes in Europe in light of the CJEU ruling of 21 December 2016 in the Joined Cases C-203/15 and C-698/15 – Report. *Eurojust* [online]. 2017 [accessed 8 May 2018]. Available from: http://data.consilium.europa.eu/doc/document/ST-10098-2017-INIT/en/pdf.

50 Eurojust Report (note 49), p. 6; A further issue, present already in the original Directive, is the reasoning behind the selection of a particular length of the retention period, now being dispersed into the many national regimes without any significant unifying rationale on EU level. Commission claimed in 2013 that most requests in practice were made within 6 months, with a minority within 12 months, see LEISER, M. – MURRAY, A.: The Role of Non-State Actors and Institutions in the Governance of New and Emerging Digital Technologies. In BROWNSWORD, R. – SCOTFORD, E. – YEUNG, K. (eds.): *The Oxford handbook of law, regulation and technology*. New York, NY: Oxford University Press, 2017, p. 689–690.

51 *Tele2/Watson*, para 108.

52 Eurojust Report (note 49), p. 6.

53 *Pl. ÚS 24/10*, para 46.

54 *Pl. ÚS 24/10*, para 47.

55 Ibid.

56 *Pl. ÚS 24/10*, para 50.

57 But see the 'obiter dictum' part in *Pl. ÚS 24/10*, paras 55–59 and see note 9.

The current provisions of the Electronic Communications Act (which were not subsequently amended after *Digital Rights Ireland*) provide for a data retention obligation along the lines of the Data Retention Directive: legal or natural persons securing public communication networks or providers of publicly available communications services are required for a period of 6 months to retain traffic and location data generated or processed in the course of providing/securing the service or network, with qualification made (in line with the Directive) for content of communication and unsuccessful calls.[58] No other qualifications limiting the scope of the data retained are present.

It is clear that if the judgement of *Tele2/Watson* is to be taken literally, such a provision is clearly in breach of the prohibition on general and indiscriminate retention of communications data (which in itself should be enough for it to be incompatible with EU law). What is more, the Czech Republic was classified by Eurojust into a group of Member States, whose legislation does not correspond with the requirement of at most targeted retention of communications data (but as was noted above, no country still keeping a data retention obligation was apparently compliant with that standard),[59] but that have not even started a reassessment of their frameworks since the judgement.[60]

It seems clear then that within the two sets of issues presented by the judgements, progress is being made in their implementation, but, only in one of them; the key problematic issue in complying with the CJEU judgements (whilst keeping some form of data retention) lies in the transition from general and indiscriminate retention of data to the 'targeted retention' model mentioned by the Court in Tele2/Watson.

As the Fundamental Rights Agency Report states, while Member States remain hesitant to implement the judgements, the number of proceedings against national data retention laws also decreased; nonetheless, the Czech data retention framework has recently been put under a challenge before the Constitutional Court, where a group of Members of the lower chamber of the Czech Parliament challenged *inter alia* the constitutionality of Art. 97 (3) and (4) of the Electronic Communications Act.[61]

---

[58] Art. 97 (3) of Act no. 127/2005 Coll., on electronic communications and amending certain related acts (Electronic Communications Act); translation of provisions author's own, as well as responsibility for any incoherences with the Czech version; para 4 of the Article further defines traffic and location data as data leading to the identification of source and addressee as well as the date, time, means, and duration of communication.

[59] See note 49; it should be mentioned that even the countries that reported a repeal of their original data retention obligations have no data retention for law purposes only, but still may (and do) rely on data collected by private operators for private (i.e. business or commercial purposes).

[60] See Eurojust Report (note 49), p. 22; A study by the NGO Privacy International, however, points to a Council document (though a copy published by Statewatch) in which the Czech Republic submitted that the judgement of *Tele2/Watson* was being followed, with the exception of targeted retention, the solution of precise implementation of which was unclear: http://data.consilium.europa.eu/doc/document/ST-6726-2017-REV-1/en/pdf [cit. 2018-05-08].

[61] The challenge was filed in December 2017 in the case Pl. ÚS 45/17; the details (including the submission on part of applicants) are available at: https://www.usoud.cz/projednavane-plenarni-veci/pl-us-4517/ [cit. 2018-05-08]; the applicants largely refer to the two CJEU judgements as well as *Pl. ÚS 24/10* in claiming precisely the unconstitutionality of general and indiscriminate retention of data whilst challenging several provisions in other laws, citing other reasons (incl. apparent lack of proper judicial oversight in some cases as well as still too wide a definition of crimes investigation of which warrants access).

4. TO REINVENT OR TO CIRCUMVENT: THE BROADER IMPLICATIONS OF DATA RETENTION RULINGS

As was stated above, the outcome of *Tele2/Watson* is a prohibition on general and indiscriminate retention of communications data such as the one in the invalidated Directive and national legislation implementing it on a similar scale; on the other hand, Member States may introduce legislation providing for targeted retention, which however 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* […]. *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.'*[62] In *Opinion 1/15*, however, the Court examined the scope of PNR data retained pursuant to the negotiated EU-Canada PNR Agreement, noting that the Agreement: *'*[…] *permits the systematic and continuous transfer of PNR data of all air passengers flying between the European Union and Canada.'*[63] Furthermore, it found that *'taken as a whole,* [*PNR data*]*, inter alia, reveal a complete travel itinerary, travel habits, relationships existing between air passengers and the financial situation of air passengers, their dietary habits or state of health, and may even provide sensitive information about those passengers*[.]*'*[64] While (as has been stated above) the wording of the agreement was not detailed enough for the Court concerning delimiting the data covered by retention, the Court did not take issue with the scope of the data retention obligation concerning its generality within the context of PNR and not electronic communications data.[65]

This means that data retention measures concerning data other than electronic communications data[66] could be subject to a slightly less stringent scrutiny (or at the very least, an examination of whether the same approach as in the two judgements is warranted in a given context) – in practice, this could be rather easily applied if the Czech Republic became a part of a sharing system of intra-EU flights PNR data pursuant to the PNR Directive.[67] Consequently, it is primarily the retention of communications data that ought to undergo a fundamental change in approach.

The Court, as well as reports, have stated several times that the use of communications data is a valuable tool in the fight against serious crime and Member States consider

---

62 *Tele2/Watson*, para 111.

63 *Opinion 1/15*, para 127.

64 *Opinion 1/15*, para 128; compare with note 18 and the notion of *'very precise conclusions'* about an individual.

65 Compare two sections of *Opinion 1/15* in paras 155–163 and 186–189; note also that sensitive data, however, deserve higher protection, and transfer and retention of them is precluded under the conditions of the case according to the Court (see para 167); For further commentary, see VEDASCHI, A. – GRAZIANI, Ch.: PNR Agreements between Fundamental Rights and National Security: Opinion 1/15. In *European Law Blog* [online] 2018 [accessed 20 August 2018] Available from: http://europeanlawblog.eu/2018/01/23/pnr-agreements-between-fundamental-rights-and-national-security-opinion-115/.

66 Retained in a way similar to the situation caused by Data Retention Directive.

67 See Art. 2 of Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (OJ L 119, 4 May 2016, p. 132–149).

it as well.[68] The effects of the use of retained data in law enforcement have, however, also been questioned on the lack of improvement of crime rates[69] and the possibility to circumvent the measure through e.g. anonymised SIM cards.[70] The switch to 'targeted retention' brings a completely new challenge: general and indiscriminate retention of data provided for a large set of data going to the past that could be analysed with the potential of discovering new connections or information that would have otherwise not been noticed.[71] This is a prime example of a situation where the methods of the so--called big data analysis can be put to use, potentially giving an enhanced perspective to investigations.[72] Instead, Member States (unless they want to give up their data retention measures) are required to switch to a method which seems to be less effective, notwithstanding the issues with the use of geographical criteria.[73] Law enforcement may thus have to adapt to using vastly different tools other than what was possible so far, and possibly reinvent certain approaches to investigation of serious crime.

---

68 See *Digital Rights Ireland*, para 43 (noting that Justice and Home Affairs Council *'*[…]*concluded that data relating to the use of electronic communications are particularly important and therefore a valuable tool in the prevention of offences and the fight against crime, in particular organised crime.'*) or FRA Report (note 47), p. 162; Nonetheless, even prior to the invalidation of the Directive, the question of evidence for such a claim was raised several times. See JONES, CH. Content and implementation of the Data Retention Directive. In: *EU Law Analysis Blog* [online] 2014 [accessed 24 August 2018] Available from: http://eulawanalysis.blogspot.com/2014/04/implementation-of-data-retention.html and the discussion of Commission reports on both quantitative and qualitative evidence of use of data retention. After the judgement, looking for such evidence is harder as there is no central piece of legislation but rather many remaining national regimes.

69 *Pl. ÚS 24/10*, para 56 as well as the submission in the current proceedings before the Czech Constitutional Court (see note 61) see p. 17–19 of the submission. On the other hand, on this ground, it should be carefully distinguished between comparing the use of retained data (designed for investigations of serious crime) against *general* crime rates (in *Digital Rights Ireland*, para 49 the Court speaks of giving national authorities *'*[…] *additional opportunities to shed light on serious crime* […]*'*) instead of a tool to in itself reduce crime rates.

70 *Pl. ÚS 24/10*, para 56 as well as the submission in the current proceedings before the Czech Constitutional Court (see note 61) see p. 17–19 of the submission; on this ground, the Court itself accepted that possibilities of circumvention do not deprive data retention of its suitability to achieve its aims (see *Digital Rights Ireland*, para 50).

71 Note in particular the comparison made by Advocate General in *Tele2/Watson*, paras 179–180: *'*[…] *Targeted surveillance measures are focused on persons who have already been identified as being potentially connected, even indirectly or remotely, with a serious crime. Such targeted measures enable the competent authorities to access data relating to communications effected by such persons, and even to access the content of their communications. However,* [*access to their communications*] *will be limited only to communications effected after the persons have been identified.* […] *General data retention obligations* […] *enable competent authorities to access the communications history of persons who have not yet been identified as being potentially connected with a serious crime. It is in this sense that general data retention obligations give law enforcement authorities a certain ability to examine the past, allowing them to access communications effected by such persons before they have been so identified.'*

72 COUDERT, F.: In the aftermath of Tele2 and Opinion 1/15: when are data retention measures legitimate? In: *KU Leuven CITIP Blog* [online]. 2017 [accessed 10 May 2018]. Available from: https://www.law.kuleuven.be/citip/blog/in-the-aftermath-of-tele2-and-opinion-115-when-are-data-retention-measures-legitimate/.

73 Ibid. See also *Pl. ÚS 24/10*, para 55, where reference is made to freezing of data pursuant as an alternative to general retention. Furthermore, see the last paragraph in LYNSKEY, O.: Tele2 Sverige AB and Watson et al: Continuity and Radical Change. In *European Law Blog* [online]. 2017 [accessed 10 May 2018]. Available from: https://europeanlawblog.eu/2017/01/12/tele2-sverige-ab-and-watson-et-al-continuity-and-radical-change/.

The resulting situation is partly described in the second part of this article: the majority of Member States still retain legislation which is contrary to the rulings, and changes are made primarily on issues other than the general and indiscriminate scope. The other consequence of these developments can be seen in new potential initiatives to re-introduce some form of broad data retention, with a recent example in the field of fighting against terrorism being called an attempt at circumvention of the *Digital Rights Ireland* and *Tele2/Watson* rulings.[74]

5. CONCLUSION

The rulings of the Court of Justice in *Digital Rights Ireland* and *Tele2/Watson* show that the Court is willing to subject interferences with fundamental rights protected by the Charter of Fundamental Rights of the EU to very strict scrutiny and review in detail various aspects of data retention regimes. The effect of these cases is twofold – first, as described in the second part of this article, immediate reaction to the rulings and the need to implement the findings into practice which after *Tele2/Watson* implies repealing national frameworks providing for general and indiscriminate retention of communications data; second, as was the subject of the third part, the rulings on the permissible scope of retention of communications data require a more thorough reassessment of the procedures involved in the fight against serious crime.

Tomáš Ochodek
Právnická fakulta Univerzity Karlovy
tomas.ochodek@seznam.cz

[74] LUND, J.: EU Member States plan to ignore EU Court data retention rulings. In *EDRi* [online]. 2017 [accessed 10 May 2018]. Available from: https://edri.org/eu-member-states-plan-to-ignore-eu-court-data-retention-rulings/.