Council of the European Union

Brussels, 1 February 2017
(OR. en)

5884/17

LIMITE

JUR 58
JAI 83
DAPIX 36
TELECOM 28
COPEN 27
CYBER 14
DROIPEN 12

INFORMATION NOTE

From:	Legal Service
To:	Permanent Representatives Committee (Part 2)
Subject:	Judgment of the Court of 21 December 2016 in joined Cases C-203/15 and C-698/15 (*Tele2 and Watson*) - Requests for a preliminary ruling concerning the interpretation of Article 15(1) of the e-privacy Directive (2002/58/EC) - Compatibility with EU law of national legislations on general data retention for the purpose of fighting crime

I. INTRODUCTION

1. By its judgment of 21 of December 2016, the Court of Justice (Grand Chamber) ruled on the requests for a preliminary ruling made by the Administrative Court of Appeal, Stockholm, Sweden (Case C-203/15, *Tele2*) and the Court of Appeal, Civil Division, England and Wales, United Kingdom (Case C-698/15, *Watson and others*). The two cases were joined. As these were interpretation cases without an invalidity issue being raised, the Council did not intervene in the proceedings, but given the importance of this judgment, an information note was warranted.

2. The invalidation in the 2014 *Digital Rights* judgment[1] of the 2006 Data Retention Directive (2006/24/EC) gave rise to questions in the Member States, in particular as regards the fate of their national transposition legislation and the availability of electronic communication data collected for access by law enforcement authorities and their use as evidence in criminal proceedings.

Member States found themselves in a situation where they no longer had an obligation deriving from a specific Union legal instrument to introduce or maintain a national data retention regime providing for the mandatory storage of electronic communication data by providers for the purposes of detecting, investigating, and prosecuting serious crime including terrorism.

However, Member States retained the possibility to do so under Article 15(1) of the e-privacy Directive,[2] subject to the fundamental rights to privacy and data protection. One of the questions was whether in doing so, Member States had to comply with the *Digital Rights* jurisprudence, and more particularly with one of the most contentious point of the judgment (point 59) where the Court had ruled that, in order to comply with the strict necessity test, the data retained should be restricted to data pertaining to a particular time period and/or a particular geographical area and/or to a circle of particular persons likely to be involved in a serious crime. This requirement was considered as, in effect, ruling out any possibility to provide for a general retention obligation for fighting crime.

3. In the present cases the Court was asked by the Swedish court (Case C-203/15, *Tele2*), in essence, to rule on whether the general and indiscriminate retention of electronic communications data is per se incompatible with the Charter or whether the compatibility of such retention of data is to be assessed in the light of provisions relating to access to the data, the protection and security of the data and the duration of retention (see point 50).

---

1 Joined Cases C-293/12 and C-594/12, judgment of 8 April 2014 (see CLS information note to Coreper of 5 may 2014, doc. 9009/14).

2 Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (OJ L 201, 31.7.2002, p. 37).
Article 15(1) reads: "*Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this 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. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union*".

The Court was asked by the British court (Case C-698/15, *Watson*), in essence, whether the *Digital Rights* judgment, and notably its points 60 to 62, lay down mandatory requirements of EU law applicable to a Member State's domestic regime on access to data retained in accordance with national legislation.[3]

II. SUMMARY OF THE JUDGMENT

The first question in Case *Tele2* (C-203/15) (whether a general data retention regime is per se incompatible with the Charter)

4. Before replying the first question, the Court examined whether the national data retention regime in question, as it makes use of the derogation allowed by Article 15(1) of the e-privacy Directive, falls within the scope of EU law and therefore implements EU law within the meaning of Article 51(1) of the Charter.

5. The Court considered that, even if Article 1(3) of the e-privacy Directive excludes from its scope activities of the State in fields like criminal law, public security, defence and State security (point 69), the measures referred to in Article 15(1) of the e-privacy Directive fall within its scope "*otherwise that provision would be deprived of any purpose. Indeed, Article 15(1) necessarily presupposes that the national measures referred to therein* (...) *fall within the scope of that directive, since it expressly authorises the Member States to adopt them only if the conditions laid down in the directive are met*" (point 73).

This makes the Charter, as interpreted by the Court notably in its *Digital Rights* judgment, applicable to such national regimes both regarding retention of data and regarding access to data by public authorities on security grounds (points 74 to 81).

[3] The difference on the content of the questions addressed to the Court is linked to the differences between the two national systems of data retention in question: the Swedish legislation provides for a general obligation of retention, while the UK legislation is based on a discretionary power of the Secretary of State.

6. In interpreting the principle of confidentiality of communications as established by the e-privacy Directive, the Court noted that, under Article 6 of the Directive, "*the processing and storage of data are permitted only to the extent necessary and for the time necessary for the billing and marketing of services and the provision of value added services*" and that "*as regards, in particular, the billing of services, that processing is permitted only up to the end of the period during which the bill may be lawfully challenged or legal proceedings brought to obtain payment. Once that period has elapsed, the data processed and stored must be erased or made anonymous*" (point 86).

7. In interpreting Article 15(1) of the e-privacy Directive, the Court stated, in line with its previous case law, that, insofar as it "*enables Member States to restrict the scope of the obligation of principle to ensure the confidentiality of communications and related traffic data,* (…) *that disposition must* (...) *be interpreted strictly* (...)*. That provision cannot, therefore, permit the exception to that obligation of principle* (...) *to become the rule, if the latter provision is not to be rendered largely meaningless*" (point 89, emphasis added).

8. The Court then examined the compatibility of the data retention obligation imposed on providers not only with the data protection provisions of the Charter (Articles 7 and 8) but also with its freedom of expression provision (Article 11) which it says "*constitutes one the essential foundations of a pluralist, democratic society and is one of the values on which, under Article 2 TUE, the Union is founded*" (points 92 and 93), an examination which it did not make in *Digital Rights*.

   The Court confirmed its previous jurisprudence in *Digital Rights* by stating that the interference entailed in the contested legislation with the above fundamental rights "*is very far reaching*", "*particularly serious*" and likely to cause a feeling of being "*subject to constant surveillance*" (point 100) and that given that seriousness, "*only the objective of fighting serious crime is capable of justifying such a measure*" (point 102). It, however, considered that as the retention did not concern the content of the communications, it did not affect the essence of the fundamental rights (point 101).

The Court then confirmed, in particular, point 59 of its *Digital Rights* judgment, ruling that, since the legislation does not restrict the retention of data in relation to a particular time period and/or geographical area and/or a group of persons likely to be involved in serious crime, its "*exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society*" (points 106 and 107).

9. The Court, however, ruled that the Charter "*does not prevent Member States 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*" (point 108, emphasis added). Such preventive retention of data must meet objective criteria that establish a connection between the data retained and the objective pursued and the conditions set in the national legislation must be such as to circumscribe in practice the extent of the preventive measure and thus the public affected. In exemplifying how to set such limits, the Court refers to "*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* [serious criminal] *offences*" (points 110 and 111).

10. The Court concluded, concerning the first question in *Tele2* (Case C-203/15) "*that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication.*" (point 112 and point 1 of the operative part of the judgment).

The second question in Tele2 (C-203/15) and the first question in Watson (C-698/15) (whether points 60 to 68 of the *Digital Right* judgment are mandatory)

11. In replying to these questions, the Court listed the different necessary safeguards that a data retention legislation should provide, insisting notably on allowing access solely for the purpose of fighting serious crime, with prior review by a court or an independent administrative authority, access only to individual suspects (save for situations where vital national security, defence or public security interests are threatened by terrorist activities), the obligation to notify the persons affected as soon as this is no longer liable to jeopardise the investigations and the obligation to irreversibly destroy the data at the end of the retention period. The Court also confirmed, as part of the obligation to ensure the full integrity and confidentiality of the retained data, the obligation to retain that data within the European Union (points 114 to 123).

12. The Court considered, however, that "*it is the task of the referring courts to determine whether and to what extent the national legislation at issue in the main proceedings satisfies the requirements stemming from Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, as set out in paragraphs 115 to 123 of this judgement, with respect to both the access of the competent national authorities to the retained data and the protection and level of security of that data*" (point 124).

III. CONSEQUENCES OF THE JUDGEMENT FOR THE COUNCIL

13. This judgment will have consequences on national data retention schemes in other Member States, which are considered to be an important tool in the fight against serious crime including terrorism. Existing national laws will need to be checked against this judgment, although this is likely to be difficult.

    It is however clear from the operative part of the *Tele2* judgment that a general and indiscriminate retention obligation for crime prevention and other security reasons would no more be possible at national level than it is at EU level, since it would violate just as much the fundamental requirements as demonstrated by the Court's insistence in two judgements delivered in Grand Chamber.

14. On 11 January 2017, the Commission tabled a proposal for a new e-privacy Regulation to replace the e-privacy Directive, which aims at aligning the regime to that of the recent Data Protection Regulation. This proposal does not longer contain a specific provision similar to Article 15(1) of the e-privacy Directive, but a new provision (Article 11), more generally worded, on possible restrictions to the basic principles - such as confidentiality and erasure of data - set out in the Regulation, which is similar to the same provision in the Data Protection Regulation (Article 23), i.e. leaving an option for the EU and Member States, subject to the Charter. The proposal also allows, as the e-privacy Directive, providers of electronic communications to process (and therefore also to retain) metadata if necessary for billing, calculating interconnection payments, and the like (see Articles 6(2)(b) and 7(3) of the proposal).

15. This judgment will of course have to be born in mind in all legislative or international negotiation activities of the Council which may involve retention, access or transfer of mass data of unsuspected persons.