COUNCIL OF THE EUROPEAN UNION

Brussels, 5 May 2014 (OR. en)

9009/14

LIMITE

JUR 249
DAPIX 58
TELECOM 106
COPEN 124

INFORMATION NOTE

From:	General Secretariat of the Council
To:	Permanent Representatives Committee/Council
Subject:	Judgment of the Court of 8 April 2014 in joined Cases C-293/12 and C-594/12 - Invalidation of 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 (the Data Retention Directive)

I. INTRODUCTION

1. By its judgment of 8 of April 2014, the Court of Justice (Grand Chamber) declared the Data Retention Directive invalid. Given that the Court has not limited the temporal effect of its judgment, the invalidity takes effect *ab initio*, i.e. from the date the Directive took effect in 2006.[1]

[1] It is recalled that this Directive had already been the subject of a judgment of the Court, but only as regards the choice of its legal basis, which was upheld by the Court (see Judgment of 10 February 2009, Case C-301/06, Ireland v. European Parliament and Council, Rec 2009 p. I-593). In point 57 of that judgment, the Court had however hinted at the issue of fundamental rights by stating that "*it must also be stated that the action brought by Ireland relates solely to the choice of legal basis and not to any possible infringement of fundamental rights arising from interference with the exercise of the right to privacy contained in Directive 2006/24*".

2. The Data Retention Directive obliges Member States to provide for an obligation for providers of publicly available electronic communications services and of public communications networks to retain traffic and location data for a period between six months and two years, the choice of the length of the period being left to each Member State in its national law.

The retention is to be performed in order to ensure that the data are available for the purpose of the investigation, detection, and prosecution of serious crime, as defined by each Member State in its national law.

II. SUMMARY OF THE JUDGMENT

3. The Court followed the usual line of reasoning which applies when examining whether certain provisions of EU law interfere with fundamental rights and if so, whether that interference is or not justified in accordance with the conditions set out in Article 52(1) of the Charter.

Existence of an interference with the rights guaranteed by Articles 7 (respect for private life) and 8 (personal data protection) of the Charter

4. The Court first stated that the obligation imposed by the Data Retention Directive to retain the data in question "*constitutes in itself an interference with the rights guaranteed by Article 7 of the Charter*" and that the access of the competent national authorities to the data and the processing of such data constitute a further interference with that right as well as "*with the fundamental right to the protection of personal data guaranteed by Article 8 of the Charter*" (points 34 to 36).

5. The Court stated that the interference in question is "*wide-ranging, and it must be considered to be particularly serious*" and that "*the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance*" (point 37, emphasis added).

Justification of the interference

6. The Court then went on to analyse whether the interference could be justified in accordance with the conditions set out in Article 52(1) of the Charter which allows limitations to fundamental rights provided that such limitations, in addition to being provided for by law,:

- respect the essence of the rights;
- genuinely meet objectives of general interest recognised by the Union; and
- subject to the principle of proportionality, are necessary.

7. As concerns the essence of the rights at stake, the Court held that "*even though the retention of data required* (…) *constitutes a particularly serious interference with* [the right to private life], *it is not such as to adversely affect the essence of those rights given that* (…) *the directive does not permit the acquisition of knowledge of the content of the electronic communications as such*" (point 39, emphasis added). This is true also with regard to the right to personal data protection as the Directive provides that certain principles of data protection and data security must be respected, notably through technical and organisational measures against accidental or unlawful destruction, accidental loss or alteration of the data (point 40).

8. As concerns whether the interference satisfies an objective of general interest, the Court upheld the general approach of data retention as a tool to fight terrorism and serious crime and thus to protect public security. It held that "*the retention of data for the purpose of allowing the competent national authorities to have possible access to those data* (…), *genuinely satisfies an objective of general interest*" (point 44, emphasis added), recalling that "*Article 6 of the Charter lays down the right of any person no only to liberty, but also to security*" (point 42).

Proportionality and necessity

9. The Court then turned to the analysis of the proportionality and necessity tests. Having recalled the main elements of the principle of proportionality, i.e. the measure should be appropriate for attaining the legitimate objectives pursued and should not exceeds what is appropriate and necessary to achieve such objectives (point 46), the Court underlined that "*where interferences with fundamental rights are at issue, the extent of the EU legislature's discretion may prove to be limited, depending on a number of factors, including, in particular, the area concerned, the nature of the right at issue guaranteed by the Charter, the nature and seriousness of the interference and the object pursued by the interference*" (point 47, emphasis added). The assessment of the principle of proportionality under Article 52(1) of the Charter is therefore more strict than the one under the general principle of proportionality set out in Article 5(4) TEU.

10. On the first element of the proportionality test, i.e. the appropriateness for attaining the objective pursued, the Court, as above, upheld data retention as an appropriate tool by holding that "*having regard to the growing importance of means of electronic communication, data which must be retained pursuant to* [the] *directive allow the national authorities which are competent for criminal prosecutions to have additional opportunities to shed light on serious crime and, in this respect, they are therefore a valuable tool for criminal investigations. Consequently, the retention of such data may be considered to be appropriate for attaining the objective pursued by that directive*" (point 49, emphasis added).

11. However, on the second element of the test, i.e. the necessity of data retention, the Court stated that, although the fight against serious crime, in particular against organised crime and terrorism, is indeed of the utmost importance, "*such an objective of general interest, however fundamental it may be, does not, in itself, justify a retention measure such as that established by Directive 2006/24 being considered to be necessary for the purpose of that fight*" (point 51).

12. The Court continued its detailed examination of the necessity test by first stating that personal data protection is especially important for the right to respect for private life and that derogations or limitations to it "*must apply only in so far as strictly necessary*" (points 52 and 53, emphasis added).

13. It is recalled that when it adopted the Data Retention Directive, the EU legislature, notably because the Directive was based on the internal market legal basis (then Article 95 TEC, now Article 114 TFEU), and not on a ex-third pillar legal basis, had limited itself to providing the obligation of data retention by the operators in order to ensure the availability of the data for the fight against terrorism and serious crime, to setting out a retention period between six months and two years (the choice being left to Member States) and to setting out general principles on access and use by law enforcement authorities, the types of crimes concerned, data protection and security, etc., without harmonising these elements in more details. The Directive left it for each Member State to provide for the necessary detailed guarantees in its national transposition law.[2]

14. Given the seriousness of the interference with the rights at stake, the Court considered that, by limiting itself to such general principles, the EU legislature exceeded the limits imposed upon it by the principle of proportionality. In such circumstances, the EU legislation in question should have laid down ""*clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data"* (point 54, emphasis added), the need for such safeguards being "*all the greater where personal data are subjected to automatic processing and where there is a significant risk of unlawful access to those data*" (point 55).

The Court particularly underlined the magnitude of the data retention which concerns "*all traffic data concerning fixed telephony, mobile telephony, Internet access, Internet e-mail and Internet telephony*". This entails "*an interference with the fundamental rights of practically the entire European population*" (point 56), covers "*in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime*" and therefore "*affects, in a comprehensive manner, all persons using electronic communications services, but without the persons whose data are retained being, even indirectly, in a situation which is liable to give rise to criminal prosecutions. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime"* (point 58, emphasis added).

[2] It is recalled that the transposition did not go easily in certain Member States, as a number of national constitutional courts annulled the national transposition laws for being contrary to the Constitution or the European Convention on Human Rights and certain national parliaments raised serious concerns.

15. The Court then lists the different defects of the Data Retention Directive which, by implication, illustrates what the Directive should have regulated to comply with the Charter (all emphasis is ours):

(a) the Directive "*does not provide for any exception, with the result that it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy*" (point 58);

(b) the Directive "(…) *does not require any relationship between the data whose retention is provided for and a threat to public security and, in particular, is not restricted to a retention in relation (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences*." (point 59);

(c) the Directive "(…) *fails to lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences that* (…) *may be considered to be sufficiently serious to justify such an interference* (…)" (point 60). More specifically on conditions for access to and use of the data, the Directive:

- "*does not contain substantive and procedural conditions relating to the access* (…) *to the data and to their subsequent use*" and "*does not expressly provide that* [access and use] *must be strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating thereto*" (point 61);
- does not either "*lay down any objective criterion by which the number of persons authorised to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued. Above all, the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions* " (point 62);

(d) the Directive requires a data retention period of at least six months "*without any distinction being made between the categories of data* (…) *on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned*" (point 63). The Directive does not state either "*that the determination of the period of retention must be based on objective criteria in order to ensure that it is limited to what is strictly necessary*" (point 64);

16. On the basis of the above analysis, the Court already concluded that the Data Retention Directive is in breach of the necessity principle, in that it "*does not lay down clear and precise rules governing the extent of the interference with the fundamental rights*" at stake and that it "*entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary*" (point 65).

Security and protection of the data retained and control by independent authorities

17. The Court however continued its examination into the rules on the security and the protection of the data retained, stating that the Directive "*does not provide for sufficient safeguards* (…) *to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data*" (point 66). This is due to the fact that the Directive:

(a) "*does not lay down rules which are specific and adapted to (i) the vast quantity of data whose retention is required* (…)*, (ii) the sensitive nature of that data and (iii) the risk of unlawful access to that data, rules which would serve, in particular, to govern the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity and confidentiality*" (point 66);

(b) "*does not ensure that a particularly high level of protection and security is applied by the providers by means of technical and organisational measures, but permits those providers in particular to have regard to economic considerations when determining the level of security which they apply, as regards the costs of implementing security measures. In particular,* [the Directive] *does not ensure the irreversible destruction of the data at the end of the data retention period*" (point 67).

18. Finally, the Court added that the Data Retention Directive "*does not require the data in question to be retained within the European Union, with the result that it cannot be held that the control, explicitly required by Article 8(3) of the Charter, by an independent authority of compliance with the requirements of protection and security* (…) *is fully ensured. Such a control, carried out on the basis of EU law, is an essential component of the protection of individuals with regard to the processing of personal data*" (point 68).

III. CONSEQUENCES OF THE JUDGMENT FOR THE COUNCIL

19. This judgment of the Court delivered by its Grand Chamber, is clearly of crucial importance in view of further action of the Union in the field of privacy and data protection. It confirms that the Court of Justice will not satisfy itself with anything less than a strict assessment of the proportionality and necessity of measures that constitute serious restrictions to fundamental rights, however legitimate the objectives pursued by the EU legislature.

It also indicates that such measures do not stand a serious chance of passing the legality test unless they are accompanied by adequate safeguards in order to ensure that any serious restriction of fundamental rights is circumscribed to what is strictly necessary and is decided in the framework of guarantees forming part of Union legislation instead of being left to the legislation of Member States.

20. The requirement of a high level of protection applies with particular strength in cases where EU legislation foresees mass data collection, storage of the data of a very large number of unsuspected persons and access to and use of such data by law enforcement authorities[3].

21. It will be for the Commission, in accordance with its right of initiative, to take the necessary steps stemming from the judgment of the Court as regards existing, proposed and future legislation of the European Union on data protection.

---

[3] Examples of such provisions are the (already allowed) access by law enforcement authorities to the Visa Information System (VIS) and to EURODAC (data base of asylum seekers). Two proposals of this nature currently under examination are the draft PNR Directive, which could potentially concern the data of between 500 million to 1,5 billion persons a year (see CLS opinion in doc. 8850/11) and the draft "entry/exit" data base of all foreign travellers entering/exiting the EU which provide for the registration of the 10 finger prints of each foreign traveller and to which many delegations wish the law enforcement authorities to have access.