European Union:
ECJ Invalidates
Data Retention Directive

June 2014

The Law Library of Congress, Global Legal Research Center
(202) 707-6462 (phone) • (866) 550-0442 (fax) • law@loc.gov • http://www.law.gov

European Union: ECJ Invalidates Data Retention Directive

Theresa Papademetriou
Senior Foreign Law Specialist

SUMMARY In April 2014, the Grand Chamber of the European Court of Justice (ECJ) declared Directive 2006/24/EC (the Data Retention Directive) invalid on the ground that European Union legislators had exceeded the limits of proportionality in forging the Directive. In particular, the Court held that the Directive entailed serious interference with the rights to privacy and personal data protection of individuals guaranteed by the Charter of Fundamental Rights, and also failed to establish limits on access by competent national authorities, such as prior review by a judicial or an independent administrative authority. Because the ECJ did not specify otherwise, the Data Retention Directive is void *ab initio* and EU Members who have transposed the Directive into their national legal systems must ensure compliance with the ECJ's judgment.

I. Introduction

On April 8, 2014, the Grand Chamber of the Court of Justice of the European Union (ECJ) delivered a much-anticipated judgment[1] concerning the legality of Directive No. 2006/24/EC, commonly referred to as the Data Retention Directive.[2] The Directive was challenged on the grounds of infringement of the right to private life, and the right to the protection of personal data of individuals, as guaranteed in articles 7 and 8, respectively, of the Charter of Fundamental Rights of the European Union.[3]

The Data Retention Directive required the providers of publicly available electronic communications services or public communications networks to retain traffic and location data belonging to individuals or legal entities. Such data included the calling telephone number and name and address of the subscriber or register user, user IDs (a unique identifier assigned to each person who signs with an electronic communications service), Internet protocol addresses, the numbers dialed, and call forwarding or call transfer records.[4] The retention period was to last for a minimum period of six months and up to two years, and the sole purpose of processing and storing the data was to prevent, investigate, detect, and prosecute serious crimes, such as

[1] Grand Chamber, Digital Rights Ireland Ltd. (C‑293/12) v. Minister for Communications, Marine and Natural Resources, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0293&rid=1.

[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, 2006 O.J. (L 105) 54, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF.

[3] Charter of the Fundamental Rights of the European Union, 2012 O.J. (C 326) 391, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN.

[4] For a detailed description of the traffic and location data, see art. 5 of Directive 2006/24/EC, *supra* note 2.

organized crime and terrorism.[5] The content of the communications of individuals was not retained.[6]

II. Legal Framework

At the European Union (EU) level, the right to privacy and personal data protection are two distinct, fundamental human rights protected by the Treaty on European Union and the Charter of Fundamental Freedoms as well as by the legal systems of the twenty-eight EU Members. The Treaty on European Union states that every individual has the right to the protection of his/her personal data.[7] The Charter of Fundamental Freedoms, whose scope extends to everyone within the jurisdictions of the EU Members, guarantees both of these rights.[8] For their part, the EU Members, in addition to their own constitutional and other legislative safeguards on privacy, are also bound, as members of the Council of Europe, to adhere to legal obligations arising from the Convention on the Processing of Personal Data[9] and the European Convention on the Protection of Human Rights and Fundamental Freedoms.[10]

The basic features of the legal regime on the protection of personal data, as enshrined in three key pieces of EU legislation, are described below.

Pursuant to Directive No. 95/46/EC on personal data protection,[11] the ownership of personal data belongs to individuals who have legal rights over the collection and processing of personal data. One of the key requirements for the processing of personal data is that the data subject must unambiguously give his/her consent, after being informed that his/her data will be processed.[12]

The processing of "sensitive" personal data that reveal ethnic or racial origin, political or religious beliefs, or memberships in unions, and the processing of data related to health and sexual orientation, is generally prohibited, except in certain instances where the data subject has consented to the processing or where processing is necessary to protect his/her vital interests.[13]

---

[5] *Id*. arts. 6 and 1, para. 1.

[6] *Id*. art. 5, para. 2.

[7] Consolidated Versions of the Treaty on European Union and the Treaty on the Functioning of the European Union, 2012 O.J. (C 326) 1, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012E/TXT.

[8] Charter of the Fundamental Rights of the European Union, 2012 O.J. (C 326) 391, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN.

[9] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, ETS, No. 108 (1981), http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm. *See also* Additional Protocol to the Convention (2001), http://conventions.coe.int/Treaty/en/Treaties/Html/181.htm.

[10] Convention for the Protection of Human Rights and Fundamental Freedoms, *as amended by* Protocols No. 11 and No. 14, ETS, No. 5 (1950), http://conventions.coe.int/treaty/en/treaties/html/005.htm.

[11] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

[12] *Id*. art. 7(a). Article 7 also includes other grounds that make the processing legitimate.

[13] *Id*. art. 8(2)(a)–(e).

Directive 2002/58/EC on personal data processing and privacy protection was enacted to guarantee the right to privacy and the protection of personal data in the electronic communications sector.[14] The Directive requires providers of publicly available electronic communications to ensure, *inter alia*, that personal data can be accessed only by authorized personnel and to also safeguard personal data that are stored or transmitted against accidental or unlawful destruction or loss, or unauthorized access, processing, or disclosure.[15]

EU Members are required to ensure the confidentiality of telecommunications and traffic data through national legislation. The Directive lists certain actions that must be prohibited by Member States, such as listening, tapping, storage, or other forms of interception by individuals (other than the users themselves) without the consent of the users, except in cases where individuals are legally authorized to do so.[16] Any restrictions imposed on established rights and obligations must be justified as necessary, appropriate, and proportionate within a democratic society and serve specific public order purposes, such as national security, defense, or public security, and the prevention, investigation, and prosecution of serious crime.[17]

Another important requirement of Directive 2002/58/EC is the obligation by providers of public communications networks or services to erase or make anonymous stored traffic data related to subscribers when they are no longer needed.[18]

Finally, as noted above, Directive 2006/24/EC, the Data Retention Directive, requires two categories of data to be retained by operators of fixed network or mobile telephony, or Internet email and Internet telephony, for law enforcement authorities: (a) data necessary to trace and identify the source of a communication, and (b) data necessary to identify the destination of a communication.[19] Operators were obliged to retain such data for a period of six months and up to two years to investigate, detect, and prosecute serious crime.[20]

---

[14] 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, 2002 (L 201) 37, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML, *as amended by* Directive 2009/136/EC, 2009 O.J. (L 137) 11, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF.

[15] *Id*. art. 4, para. 1.

[16] *Id*. art. 15, para. 1.

[17] *Id*.

[18] *Id*. art. 6, para. 1.

[19] Directive 2006/24/EC, *supra* note 2.

[20] *Id*. arts. 1, 6.

III. Judgment of the ECJ

The case arose before the ECJ as preliminary questions from the High Court of Ireland and the Constitutional Court of Austria. The national courts, in adjudicating cases, have the right to refer legal inquires to the ECJ. The ECJ decides on the validity of European Union law, or the interpretation of treaties or secondary legislation, and the decision on the specific case is left to the national court.[21]

The High Court in Ireland had to adjudicate a dispute between the Irish company Digital Rights Ireland and the Irish authorities on the legality of national measures implementing the retention of data of electronic communications.[22] The Austrian Constitutional Court (CC) had before it several actions filed by a large number of applicants seeking the annulment of the Austrian telecommunications law that transposed the Data Retention Directive into national law. The CC took the view that the retention affected a large number of individuals whose conduct did not justify the retention of their data for such a long time and that such persons were exposed to the risk that the government authorities would become privy to the content of data and violate their privacy. The CC expressed its concern as to whether the Data Retention Directive would be able to achieve its objectives as intended without violating the principle of proportionality.[23]

In considering the broad category of data to be retained, the ECJ observed that such data

> 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 environment.[24]

The Court observed that under such circumstances, even though it is not permissible to retain the content of communications, it is possible that the freedom of expression of subscribers or registered users might be in jeopardy.[25]

The ECJ stated that the retention of data in order to allow access by the competent national authorities constitutes processing of data and therefore affects two basic rights of the Charter of Fundamental Rights: (a) the right to private life guaranteed by article 7, and (b) the protection of personal data guaranteed by article 8.[26]

In examining the issue of interference with the rights to privacy and the protection of personal data, the ECJ made the following observations:

---

[21] *Summaries of EU Legislation: The Reference for a Preliminary Ruling*, EUROPA, http://europa.eu/legislation_summaries/institutional_affairs/decisionmaking_process/l14552_en.htm (last updated Feb. 20, 2013).

[22] Digital Rights Ireland Ltd. (C‑293/12), *supra* note 1, paras. 17–18.

[23] *Id*. paras. 19–22.

[24] *Id*. para. 27.

[25] *Id*. para. 28.

[26] *Id*. para. 29.

- The obligation imposed on providers of electronic communications services or public communications networks "constitutes in itself an interference with the rights guaranteed by article 7 of the Charter,"
- Access of the national authorities to data "constitutes a further interference with that fundamental right," and
- The interferences described above also violate the right to protection of personal data.[27]

Article 52(1) of the Charter requires that any limitation on the exercise of rights guaranteed by the Charter must be provided by law and must respect the essence of such rights. Any limitations are subject to a proportionality test and can be imposed only if they are necessary and meet the objectives of general interest as recognized by the EU or the need to protect the rights and freedoms of others.

The ECJ took note of the basic objective of the Data Retention Directive, which is to assist the EU Members in their fight against serious crime and to contribute to maintaining public security. It also noted that the fight against international terrorism constitutes an objective of general interest. In this regard, it acknowledged that data retention is a valuable tool for the national authorities in their pursuit of fighting serious crime. Based on these observations, the ECJ reached the conclusion that retention of data in order to give an opportunity to national authorities to access such data for the prevention and investigation of serious crimes "genuinely satisfies an objective of general interest."[28]

In this regard, the Court stated that the EU legislation in question must contain clear and precise rules pertaining to the retention of personal data and must also include certain safeguards to ensure that individuals whose data are retained have certain guarantees to protect their personal data "against the risk of abuse and against any unlawful access and use of that data."[29]

The ECJ then proceeded to examine whether the interference by national authorities was proportionate to the objective pursued. In this regard, according to the settled case law, the standards to be met are that of being "appropriate" and "necessary" in order to achieve the objectives.

As far as the question of whether the retention of data was appropriate to achieve the objectives of Directive 2006/24/EC, the ECJ, after acknowledging that the means of electronic communication play a vital role in the investigation of crimes and at the same time the need of national authorities to access data, stated that retention of data is "a valuable tool" and "may be considered to be appropriate" to achieve the Directive's objectives.[30]

[27] *Id*. paras. 34–36.

[28] *Id*. para. 44.

[29] *Id*. para. 54.

[30] *Id*. para. 49.

As far as the necessity test, and whether the interference is limited to what is necessary, the Court made three significant observations: (a) the Directive requires the retention of all traffic data generated from a wide range of electronic communication modes, including fixed telephony, mobile telephony, Internet access, Internet email, and Internet telephony; (b) the Directive's scope extends to all subscribers and registered users; and (c) the Directive interferes with the fundamental rights of the entire European Union population.[31]

The Court went on to state that the retention of data affects not only persons whose data may contribute to the initiation of legal proceedings, but also those for whom there is not a shred of evidence to suggest that their conduct might be connected to a serious crime. It also observed that no one is exempted from this rule; it even applies to those whose communications are subject to professional secrecy, according to national rules.[32]

In further discussing the Directive, the ECJ observed the absence of any link between the data retained and a threat to public security. It also noted that the restriction is not limited to the data of persons related to a particular time period, or to a particular geographic zone, or to a group of persons who could possibly have a tie to a serious crime.

Moreover, the ECJ reviewed whether the Directive contained any general limits on the right of national authorities to access the retained data. In this regard, the ECJ observed the lack of any general limits. Then, it proceeded to state that the Directive (a) fails to establish either substantive or procedural limits on access by competent national authorities to the data retained,[33] (b) fails to make access by national authorities conditional on a prior review carried out by a court or any other independent administrative authority whose review is essential in order to limit access to the data and their use to what it is absolutely necessary, and (c) does not require the Member States to establish such limits.[34]

As far as the period of retention, which runs from six months up to two years, the ECJ noted that the Directive does not set any objective criteria to determine the appropriate period of retention "to what is strictly necessary."[35]

The Court reasoned that, based on the above, the Directive does not establish clear and precise rules that regulate the "extent of interference with the fundamental rights of Art. 7 and 8 of the Charter." Therefore, it concluded that the Directive "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 it is strictly necessary."[36]

---

[31] *Id*. para. 56.

[32] *Id*. para. 58.

[33] *Id*. paras. 59–61.

[34] *Id*. para. 62.

[35] *Id*. para. 64.

[36] *Id*. para. 65.

Regarding the security and protection of data to be retained, the ECJ held that Directive 2006/24/EC does not contain sufficient safeguards, as required by article 8 of the Charter, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data. Article 8 of the Charter requires, *inter alia*, the consent of the data subject for the processing of personal data, and processing must be done for a specific person. The Court went on to state that Directive 2006/24/EC does not contain rules

> which are specific and adapted to (i) the vast quantity of data whose retention is required by that directive, (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. Furthermore, a specific obligation on Member States to establish such rules has also not been laid down.[37]

The ECJ also held that the security and protection of personal data cannot be fully guaranteed in the absence of review of compliance by an independent authority of the rules on data protection, as required by article 8 of the Charter of Fundamental Rights.[38]

Based on the above, the ECJ concluded that the EU legislative bodies, by adopting Directive 2006/24/EC, exceeded the limits imposed by the principle of proportionality in light of articles 7, 8, and 52(1) of the Charter. Consequently, it held the Directive invalid.[39]

IV. Effect of the Judgment

The Data Retention Directive becomes invalid *ab initio*, that is from the time it became effective in 2006, since the ECJ did not specify otherwise. The EU Members that have transposed the Directive into their national legal systems are required to take steps to ensure compliance with the judgment.

In exercising its right to initiative, the European Commission will have to adhere to the ECJ's judgment when it introduces new legislation on data protection and privacy. Any pending legislation must also be in conformity with the ECJ's case law affecting personal data. In particular, the proposal for the Directive on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for purposes of addressing criminal offenses must be in conformity with the ECJ's ruling.[40]

---

[37] *Id*. para. 66.

[38] *Id*.

[39] *Id*. para. 73.

[40] *Proposal for a Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data*, COM (2012) 10 final (Jan. 25, 2012), http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_10_en.pdf.

The President of the European Parliament Martin Schulz stated as follows in response to the ECJ's ruling:

> Today's judgment must be carefully examined and the Commission will have to make a proposal which strikes the right balance between the legitimate interests at stake. Any new proposal must respect in every detail the guarantees laid down in the Charter of Fundamental Rights. It should in particular enshrine a high level of data protection – which is all the more essential in the digital age – thus avoiding disproportionate interferences with the private lives of citizens.[41]

[41] Press Release, European Parliament/The President, Schulz on the Annulment of the Data Retention Directive (Apr. 8, 2014), http://www.europarl.europa.eu/former_ep_presidents/president-schulz/en/press/press_release_speeches/press_release/2014/2014-april/html/schulz-on-the-annulment-of-the-data-retention-directive.