**Conseil d'État**
**Contentious Section**
**N° 393099: *FDN et al. c/ Gouvernement***

**Third-Party Intervention**

The Center for Democracy & Technology ('CDT'), a nonprofit corporation formed under the laws of the District of Columbia, United States of America, on 6 December 1994 (license no. 53006721), and recognized as a nonprofit corporation under Section 501(c)(3) of the United States Internal Revenue Code (employer identification no. 52-1905358),

having its place of business at 1634 I Street Northwest, Suite 1100, Washington, D.C., 20006, United States of America,

represented by its President and Chief Executive Officer, Nuala O'Connor,

- and -

Privacy International, a nonprofit organisation formed in 1990 under the laws of the United Kingdom of Great Britain and Northern Ireland, and a registered UK charity (No. 1147471)**,**

having its place of business at 62 Britton Street, London, EC1M 5UY, United Kingdom,

represented by its Executive Director, Dr Gus Hosein,

hereby request the permission of the the Conseil d'État to submit the following third-party intervention.

## I. Introduction and summary

**1.** The Center for Democracy & Technology and Privacy International are honoured to submit this third-party intervention in the case of *FDN et al. c/ Gouvernement* (n° 393099), filed before the Tenth sub-section of the Conseil d'État. The claimants in the case challenge the government's refusal to abrogate Article R10-13 of the Code of postal and electronic communications and Decree n° 2011-219 of 25 February 2011 concerning the conservation and communication of data permitting the identification of all persons who have contributed to the creation of online content.

**2.** CDT is a non-governmental organisation that works to advance human rights online, and is committed to finding forward-looking and technically sound solutions to the most pressing challenges facing users of electronic communications technologies. Since its founding more than 20 years ago, CDT has played a leading role in shaping policies, practices and norms that empower individuals to use these technologies effectively as speakers, entrepreneurs and active citizens. Based in Washington, DC, the organisation is a registered charity in the United States. CDT actively promotes the sound development of European human rights laws and norms in the areas of privacy and free expression, as well as the adherence of national laws to the European human rights framework where these issues are concerned. The organisation has previously intervened in a European Court of Human Rights case concerning government access to private data (*Szabó and Vissy v Hungary*, n° 37138/14) and has requested permission to intervene in two ECtHR cases concerning the United Kingdom's surveillance practices (*Big Brother Watch and ors v the United Kingdom*, n° 58170/13; *Bureau of Investigative Journalism and Ross v the United Kingdom*, n° 62322/14). CDT therefore submits that it has standing to intervene in this case in the public interest.

**3.** Privacy International was founded in 1990 and was the first organisation to campaign at an international level on privacy issues. The organisation is based in London and is committed to fighting for the right to privacy across the globe, including through research, litigation and advocacy. It is a registered charity in the United Kingdom and envisions a world in which the right to privacy is protected, respected and fulfilled. Privacy International is a leading authority on privacy and free expression rights, and advocates for national and regional laws that protect these rights. It has previously brought several challenges against surveillance practices in the UK courts and the ECtHR, and has intervened in Hungarian and UK cases concerning the compliance of data retention schemes with EU law (*Dalma Dojcsak v Telenor Magyarország ZRT*; *Davis and Watson v Secretary of State for the Home Department*). It therefore has standing to intervene in this case in the public interest.

**4.** Our organisations submit this brief to assist the Conseil d'État in addressing two issues: the compatibility of the challenged data-retention provisions (Article R10-13 of the Code of postal and electronic communications and Decree n° 2011-219 of 25 February 2011) with the Charter of Fundamental Rights of the European Union ('the Charter') in light of the judgment of the Court of Justice of the European Union ('CJEU') in *Digital Rights Ireland v Minister for Communications, Marine and Natural Resources et al*[1]; and the compatibility of these provisions with Article 8 of the European Convention on Human Rights ('ECHR').

**5.** We conclude that the challenged provisions are not compatible with the Charter and are therefore unlawful as a matter of EU law, and that the scope, duration, and indiscriminate nature of the mandated data retention violate Article 8 of the ECHR.

## II. The challenged data-retention provisions are not compatible with the Charter of Fundamental Rights of the European Union and are therefore unlawful under EU law

### *a. The challenged data-retention requirements implement EU law and must comply with the Charter of Fundamental Rights of the European Union*

**6.** In accordance with Article 51(1) of the Charter, France is obligated to respect the rights found in the Charter whenever it implements European Union law.[2] The CJEU's case-law indicates that not only national provisions that are intended to give effect to EU law, but also those that pursue objectives that are covered by EU law and those that could be affected by specific rules of EU law, should be regarded as falling 'in the scope' of EU law for the purposes of the Charter.[3]

**7.** For two decades, EU legislation has sought to harmonise Member States' respect for privacy rights in the context of electronic communications and the processing of personal data.[4] In doing so, the EU legislator has comprehensively regulated the processing of personal data, including by requiring the Member States to 'ensure the confidentiality of communications and related traffic data' by prohibiting, *inter alia*, 'storage or other kinds of interception of communications and the related traffic data by persons other than users, without the consent of the users concerned, except where legally authorised to do so' in accordance with exceptions

[1] Case C-293/12, joined with *Kärntner Landesregierung et al* (Case C-594/12), Judgment (Grand Chamber), 8 April 2014 (hereinafter '*Digital Rights Ireland*').
[2] Charter of Fundamental Rights of the European Union (2000/C 364/01) (hereinafter 'Charter').
[3] See *Cruciano Siragusa v Regione Sicilia – Soprintendenza Beni Culturali e Ambientali di Palermo* (Case C-206/13), Judgment, 6 March 2014, ¶ 25; Explanations Relating to the Charter of Fundamental Rights (2007/C 303/02), p. 32.
[4] See, e.g., Directive 95/46 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; Directive 2002/58 of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector; cf. *Institut professionnel des agents immobiliers (IPI) v Englebert et al* (Case C-473/12), Judgment, 7 November 2013, ¶ 28.

that are set out in in the relevant legislation.[5] Although the EU laws in this area permit Member States to derogate from this scheme on certain limited grounds, in our view there can be little question that a Member State is acting within the scope of EU law when it adopts laws or regulations concerning the treatment of personal data.[6]

**8.** Where the first of the challenged provisions, Article R10-13 of the Code of postal and electronic communications, is concerned, we note that the Ministry of Justice has explicitly confirmed that France was implementing EU law when it adopted Decree no 2006-356 of 24 March 2006 concerning the conservation of electronic communications data (which created Article R10-13).[7]

**9.** Meanwhile, the second of the challenged provisions, Decree n° 2011-219 of 25 February 2011, obligates hosting providers to retain a broad range of data—including, for example, subscriber data such as names and postal addresses—that facilitate the identification of every individual creator of or contributor to any type of online content, potentially including private communications.[8] We submit that France's treatment of such data (including by requiring its retention) is directly affected by EU legislation pertaining to the protection of personal data, which concerns the processing of 'any information relating to an identified or identifiable natural person'.[9] Thus, the Decree falls within the scope of EU law.[10]

**10.** It is therefore our view that the French provisions at issue in this case are within the scope of EU law, such that the provisions of the Charter apply.

*b. The data retention requirements at issue constitute limitations on the Charter rights to privacy and the protection of personal data*

**11.** As the Conseil d'État will be aware, the Charter establishes that when Member States are implementing EU law, they must comply with the rights to 'respect for … private and family life, home and communications' (Article 7) and the protection of personal data (Article 8).[11] The Member States are only permitted to impose limitations on these rights if such limitations comply with criteria set out in the Charter (see paragraph 17 below).[12]

**12.** In its judgment in the conjoined cases known as *Digital Rights Ireland*, the CJEU found that '*the obligation … on providers of publicly available electronic communications services or of public communications networks to retain, for a certain period,*' data necessary to identify the source and destination of a telephone or Internet communication, as well as its date, time and

---

[5] Directive 2002/58, arts. 5(1), 15(1).

[6] For permissible grounds for derogation, see Directive 95/46, art. 13. On the obligation to comply with the Charter when acting pursuant to an exception in EU law, see *Pfleger et al* (Case C-390/12), Judgment, 30 April 2014, ¶¶ 33-36.

[7] France adopted the decree in order to transpose Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, commonly known as the Data Retention Directive; see Question écrite n° 54372 de M. Lionel Tardy, 22 April 2014, available at http://questions.assemblee-nationale.fr/q14/14-54372QE.htm. As discussed below, the CJEU has subsequently invalidated the Data Retention Directive in its entirety on the grounds of its incompatibility with the Charter; however, the Court had previously confirmed that the Union legislator had had a valid legal basis for promulgating the Directive (*Ireland v European Parliament and Council of the European Union* (Case C-301/06), Judgment, 10 February 2009), meaning that in our view, France's adoption of Decree no 2006-356 of 24 March 2006 remains an implementation of EU law notwithstanding the later invalidation of the Directive on fundamental-rights grounds. Additionally, as explained in ¶ 7 above, France is implementing EU law whenever it adopts laws or regulations concerning the treatment of personal data.

[8] Decree n° 2011-219 of 25 February 2011 concerning the conservation and communication of data permitting the identification of all persons who have contributed to the creation of online content, JORF n° 0050 of 1 March 2011, p. 3643.

[9] Directive 95/46, arts. 2-3.

[10] See *supra* n. 3 and accompanying text.

[11] Charter, *supra* n. 2, arts. 7, 8 and 51(1).

[12] *Ibid.* at art. 52(1).

duration and the equipment involved, constituted an interference with the right to privacy found in Article 7 of the Charter.[13]

**13.** The Court also found that these data-retention obligations constituted an interference with the right to the protection of personal data found at Article 8 of the Charter, as they '*provide[d] for the processing of personal data*'.[14]

**14.** The Court appears to have used the term 'interference' as a synonym for 'limitation' in the sense in which the latter is employed in Article 52(1) of the Charter.[15] It characterised the interferences with privacy and data-protection rights at issue in the case as '*particularly serious*', noting 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.*'[16]

**15.** That the collection and retention of communications data constitutes an interference with the right to privacy has been recognised by a range of international bodies and human rights experts, including the Article 29 Working Party, the UN Office of the High Commissioner for Human Rights, the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, and the Council of Europe Commissioner for Human Rights.[17]

**16.** As the types of data at issue in the present case include and may even exceed those whose retention was at issue in *Digital Rights Ireland*, we believe the above findings necessitate a conclusion that the French provisions whose abrogation the claimants are seeking place limitations on the Charter rights to privacy and data protection.[18]

*c. These limitations exceed what is strictly necessary and are therefore in breach of EU law*

**17.** In accordance with the Charter, France may only limit the rights found therein if such limitations are 'necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.'[19] Meanwhile, where the State seeks to limit the '*right to respect for private life … in relation to the protection of personal data*' in particular, the limitation must meet the heightened standard of being '*strictly necessary*'.[20]

**18.** In *Digital Rights Ireland*, the CJEU found that Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, commonly known as the Data Retention Directive, interfered with privacy and data-protection rights in a manner that exceeded what was 'strictly necessary' to combat serious crime and ensure public security.[21] The Court reached this conclusion for the following reasons:

---

[13] *Digital Rights Ireland*, *supra* n. 1, ¶ 34.
[14] *Ibid.* at ¶ 36.
[15] See *ibid.* at ¶¶ 38-39 and 45.
[16] *Ibid.* at ¶ 37.
[17] Article 29 Data Protection Working Party, *Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes*, 819/14/EN, 10 April 2014; Office of the United Nations High Commissioner for Human Rights, *The right to privacy in the digital age*, A/HRC/27/37, 30 June 2014; Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Report, *Promotion and protection of human rights and fundamental freedoms while countering terrorism*, A/69/397, 23 September 2014; Council of Europe Commissioner for Human Rights, *The rule of law on the internet and in the wider digital world*, 2014.
[18] The claimants have indicated that Decree n° 2011-219 of 25 February 2011 imposes data-retention obligations on hosting services, and thus is even broader in scope than the Data Retention Directive (invalidated in *Digital Rights Ireland*) was.
[19] Charter, *supra* n. 2, art. 52(1).
[20] *Digital Rights Ireland*, supra n. 1, ¶ 52 (citing *IPI v Englebert*, *supra* n. 3, ¶ 39).
[21] *Ibid*. at ¶¶ 41 and 65.

i. the Directive '*cover[ed], 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*';[22]

ii. it did not include exceptions for '*persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy*';[23]

iii. it did not '*require any relationship between the data whose retention [was] provided for and a threat to public security*': in addition to failing to require any type of link, '*even an indirect or remote one*', between the persons affected and serious crime, it failed to place temporal or geographic limitations on the data to be retained;[24]

iv. it neglected to set out any substantive or procedural criteria governing the access of the competent national authorities to the data or limiting the number of authorities who could obtain such access;[25]

v. it did not require that access to the retained data depend 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 ... and which intervenes following a reasoned request of [the competent national] authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions*';[26]

vi. it failed to mandate that the subsequent use of the data must be confined to the prevention, detection or criminal prosecution of offences, or that these offences must be of a sufficient gravity to justify the serious interference with fundamental rights involved;[27]

vii. it did not include a requirement that the retention period '*be based on objective criteria in order to ensure that it is limited to what is strictly necessary*', or that distinctions be drawn in this regard between categories of data based on their usefulness in pursuing a legitimate aim;[28]

viii. it failed to establish sufficient safeguards to ensure the security of the data;[29]

ix. it did not mandate that the data must be irreversibly destroyed at the end of the retention period;[30] and

x. it did not require that the data be retained within the EU.[31]

**19.** In our view, the Court's inclusion of these factors indicates that each is a component of the relevant Charter rights and is therefore a requirement applying to the EU institutions and to the

---

[22] *Ibid.* at ¶ 57; see also *Schrems v Data Protection Commissioner* (Case C-362/14), Judgment, 6 October 2015, ¶ 93 ('*Legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the European Union to*' a third country '*without any differentiation, limitation or exception being made in the light of the objective pursued*').

[23] *Digital Rights Ireland*, supra n. 1, ¶ 58.

[24] *Ibid.* at ¶¶ 58-59; cf. *Schrems*, *supra* n. 22, ¶ 93 (indicating that legislation concerning the storage of personal data must set out '*an objective criterion ... by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference*' which access to and use of the data entail).

[25] *Digital Rights Ireland*, supra n. 1, ¶¶ 60-62; see also *Schrems*, *supra* n. 22, ¶ 90 (indicating that authorities' access to, and subsequent processing of, personal data must be '*strictly necessary and proportionate*' to a legitimate objective).

[26] *Digital Rights Ireland*, *supra* n. 1, ¶ 62; see also *Schrems*, *supra* n. 22, ¶ 91 (emphasising the need for '*sufficient guarantees enabling [personal] data to be effectively protected against the risk of abuse and against any unlawful access and use of that data*').

[27] *Digital Rights Ireland*, *supra* n. 1, ¶¶ 60-61; see also *Schrems*, *supra* n. 22, ¶ 93.

[28] *Digital Rights Ireland*, *supra* n. 1, ¶¶ 63-64; see also *Schrems*, *supra* n. 22, ¶ 93 (indicating that the storage of personal data should be subject to differentiation, limitation and/or exception depending on the objective pursued).

[29] *Ibid.* at ¶ 66.

[30] *Ibid.* at ¶ 67.

[31] *Ibid.* at ¶ 68. Regarding this list of the reasons upon which the Court's conclusion was based, cf. David Anderson, *A Question of Trust: Report of the Investigatory Powers Review*, June 2015, pp. 87-88.

Member States when implementing EU law. The Court's prior jurisprudence suggests that in the normal course of events, it would have invalidated each relevant individual provision of the Data Retention Directive, and that its decision to invalidate the Directive as a whole was based upon the extent to which the instrument was undermined by the specific failings the Court identified.[32] In other words, each of the characteristics described above must be viewed as violating the Charter, independently from any cumulative impact they may have.[33]

**20.** The CJEU's judgment in *Schrems v Data Protection Commissioner* provides additional confirmation that the criteria set out at points (i) and (iii)-(vii) above apply to any storage of personal data that falls within the scope of EU law, and are not limited to the specific context in which the Court applied them in *Digital Rights Ireland*.[34]

**21.** Where the compliance of the French provisions at issue in this case with the requirements of the Charter as articulated in *Digital Rights Ireland* is concerned, we defer to the claimants as to whether the access regime in place concerning the data retention mandated by these provisions meets the criteria set out at points (iv) and (v) above). We also defer to the claimants as to whether the safeguards in place to ensure the security of the data (point viii above), such as those set out in Article 34 of Law n° 78-17 of 6 January 1978 on information, files and freedoms, are sufficient.

**22.** However, we submit that Article R10-13 of the Code of postal and electronic communications exhibits, at minimum, the characteristics set out in (i)-(iii), (vi-vii) and (ix-x) above: it covers all persons, all means of electronic communication, and all traffic data without making any differentiation based on the legitimate aim pursued; it does not include any exceptions for persons whose communications are subject to an obligation of professional secrecy; it does not require any connection, of the kind set out by the CJEU, between the data to be retained and a threat to public security; it does not provide that subsequent use of the data must be confined to the prevention, detection or criminal prosecution of offences whose seriousness is sufficient to render the privacy interference proportionate; it does not ensure that the retention period is limited to what is strictly necessary based on objective criteria; and it contains no provisions to guarantee that the data is stored within the EU and is irreversibly destroyed at the end of the retention period.

**23.** Decree n° 2011-219 of 25 February 2011 exhibits the same characteristics, save that the decree applies to all means of the 'creation of online content' instead of all means of electronic communication as such.

**24.** In sum, these provisions exhibit several of the prohibited characteristics described in paragraph 18 above, and thus constitute impermissible limitations on the rights found in Articles 7 and 8 of the Charter; they are therefore in breach of EU law. We defer to the claimants as to whether other aspects of these provisions may also violate EU law.

---

[32] Cf. *Association Belge des Consommateurs Test-Achats and ors v Conseil de Ministres* (Case C-236/09), Judgment (Grand Chamber), 1 March 2011 (invalidating a specific provision of Directive 2004/113/EC on the grounds of its incompatibility with the Charter).

[33] The District Court of the Hague has reportedly concluded that the CJEU's reliance upon these factors was cumulative in nature (David Anderson, *supra* n. 31, p. 89), and the High Court of England and Wales in *Davis & Ors*, *infra* n. 67, appears to have done the same. By contrast, the Belgian constitutional court appears to have viewed the factors as severable to at least some extent (*In the matters introduced by the Francophone and German-speaking bars et al.*, Order n° 84/2015 of 11 June 2015, pp. 33-34, available at http://www.const-court.be/public/f/2015/2015-084f.pdf). As noted herein, we believe each of the factors set out by the CJEU in *Digital Rights Ireland* reflects, individually, a requirement of the Charter, and we believe the Conseil d'État must adopt such an approach. Cf. *S and Marper v the United Kingdom*, Nos 30562/04 & 30566/04, Judgment (Grand Chamber), 4 December 2008, ¶ 99 (describing as '*essential*' the existence of '*clear, detailed rules governing the scope and application of measures [for the storage and use of personal information], as well as minimum safeguards concerning,* inter alia*, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction*'). Even if the Conseil d'État does not agree, we submit that the challenged French data retention provisions are nevertheless invalid at least insofar as they exhibit the characteristics listed herein (see ¶¶ 21-23).

[34] See *supra* nn. 22, 24-28 and accompanying text.

## III. The challenged provisions violate Article 8 of the European Convention on Human Rights

**25.** Article 8 of the ECHR grants everyone in France's jurisdiction the right to respect for his or her private life and correspondence. The State may not interfere with this right except where such an interference is 'in accordance with the law and is necessary in a democratic society' to achieve one of the purposes enumerated in the Article, such as national security or the prevention of disorder or crime.[35]

**26.** The ECtHR has previously held that the collection and storage of information related to telephone communications, such as the date and length of a conversation and the number dialled, constitute interferences with the right to respect for private life even where the content of the conversation is not obtained or examined.[36] As the Court has historically treated telephone, e-mail, facsimile and other forms of communication taking place through technological means as subject to the same Article 8 protections, this holding must be assumed to extend to personal information transmitted or stored via the Internet.[37]

**27.** The Court has further confirmed that even *'[t]he mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8*', regardless of whether or how the data are subsequently used, whether they are '*sensitive*' or whether the individual is '*inconvenienced in any way*'.[38] Information concerning business, professional or even public activities may fall within the scope of 'private life', such that the State's collection and storage of data pertaining to such activities may constitute an interference with Article 8 rights.[39]

**28.** In line with the Court's case-law, even the mere existence of legislation authorising or requiring such collection and storing amounts to an interference for the purposes of Article 8, regardless of how the legislation is implemented in practice; as the Court has observed, the '*menace of surveillance ... necessarily strikes at freedom of communication between users*' of telephone and other communication services.[40]

**29.** On the basis of these precedents, we submit that the challenged French provisions, by which the State mandates the systematic collection and storage of data pertaining to all or virtually all Internet and telephonic communication, unquestionably constitute an interference with Article 8.

**30.** As the relevant activities qualify as interferences, they must, pursuant to Article 8, § 2 of the Convention, be done 'in accordance with the law' and be 'necessary in a democratic society' in order to be lawful.[41] In the context of 'secret surveillance' (a term that encompasses at least the mandatory collection, storage, searching, and use of data concerning correspondence, and—we submit—the creation of online content), the Court has specified that such interferences, '*characterising as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions*'.[42]

**31.** The ECtHR has yet to address the specific question of whether a non-targeted data retention scheme affecting virtually every telephonic or Internet communication sent or received by any individual within the Contracting Party's jurisdiction may be regarded as meeting the legality and necessity requirements imposed by Article 8, § 2. However, the Court's case-law strongly

---

[35] Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter 'ECHR'), arts. 1 and 8.

[36] *Copland v the United Kingdom*, No 62617/00, Judgment, 3 April 2007, ¶¶ 43-44; cf. *Rotaru v Romania*, No 28341/95, Judgment (Grand Chamber), 4 May 2000, ¶ 46.

[37] See, e.g., *Liberty and ors v the United Kingdom*, No 58243/00, Judgment, 1 July 2008, ¶ 56; *Kennedy v the United Kingdom*, No 26839/05, Judgment, 18 May 2010, ¶ 118.

[38] *S and Marper*, *supra* n. 33, ¶ 67; *Amann v Switzerland*, No 27798/95, Judgment (Grand Chamber), 16 February 2000, ¶¶ 69, 70.

[39] *Shimovolos v Russia*, No 30194/09, Judgment, 21 June 2011, ¶ 65; *Niemietz v Germany*, No 13710/88, Judgment, 16 December 1992, ¶¶ 29-31.

[40] See *Klass and ors v Germany*, No 5029/71, Judgment (Plenary), 6 September 1978, ¶ 41.

[41] ECHR, *supra* n. 35.

[42] *Klass*, *supra* n. 40, ¶ 42; see also *Rotaru*, *supra* n. 36, ¶ 47; *Dragojević v Croatia*, No 68955/11, Judgment, 15 January 2015, ¶ 84; *Kennedy*, *supra* n. 37, ¶ 153.

suggests that such a scheme, even when it has a legitimate aim, cannot be regarded as 'in accordance with the law' or proportionate and therefore violates the Convention.[43]

**32.** Where the legality requirement found in Article 8, § 2 is concerned, we note that the Court requires the Contracting Parties to impose restrictions on the relevant privacy interferences through statutory law, including (*inter alia*) '*the nature of the offences which may give rise*' to the interferences and '*a definition of the categories of people liable to have their communications monitored*'.[44] As a general matter, '*the law must be sufficiently clear in its terms to give citizens an adequate indication of the conditions and circumstances in which the authorities are empowered to resort to*' the surveillance.[45] Such strictures are designed to protect individuals against '*arbitrary*' interferences with their privacy.[46] Thus, the Court has found violations of Article 8 where domestic laws permitted the authorities to monitor broad or potentially broad categories of persons, particularly those who have not been involved in serious offences.[47]

**33.** Moreover, the Court has previously indicated that a monitoring scheme will not be 'in accordance with the law' if it fails to ensure that persons who are monitored are notified of the surveillance (if only *ex post facto*).[48]

**34.** We observe that each of these requirements would be rendered meaningless if the Contracting Parties were permitted to adopt data-retention schemes involving the collection and storage, for a year or even longer, of highly revealing information pertaining to virtually all communications sent, received or otherwise created by everyone within their jurisdictions. We therefore conclude that the schemes created by the French provisions at issue in this case are not 'in accordance with the law' and violate the Convention.[49]

**35.** Where the 'necessity' criterion found in Article 8, § 2 is concerned, the Court has strongly suggested that at least when communications are internal (i.e., taking place solely between persons in the Contracting State's jurisdiction), individualised warranting is required, and the nature and duration of the monitoring must similarly be limited based on the needs of the particular investigation in question.[50]

**36.** Meanwhile, while the admissibility decision of the Court's Fourth Section in *Weber and Saravia v Germany* may be read to permit some forms of 'strategic monitoring' where external communications are concerned, we note that the Fourth Section appears to have understood itself as evaluating surveillance (and the transmission of surveillance data to other authorities) that had been triggered by the use of 'catchwords' during international wireless telephone conversations; these activities, as the Fourth Section understood them, were thus of an individualised (or at least discriminate) nature and authorised only for the investigation and prevention of certain serious offenses.[51] (We make this observation without conceding that the Fourth Section's apparent view as to when the relevant interference with Article 8 rights arose was correct.) Moreover, the Fourth Section reached its conclusions in *Weber and Saravia* at a

---

[43] Pursuant to the Court's jurisprudence, an interference with the right to private life must be proportionate to a legitimate aim in order to qualify as 'necessary in a democratic society' for the purposes of Article 8, § 2 of the Convention. See generally *Leander v Sweden*, No 9248/81, Judgment, 26 March 1987, ¶ 58; *Niemietz*, *supra* n. 39, ¶ 37; *Peck v the United Kingdom*, No 44647/98, Judgment, 28 January 2003, ¶ 76.

[44] *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria*, No 62540/00, Judgment, 28 June 2007, ¶ 76; cf. *Kennedy*, *supra* n. 37, ¶ 160; *Iordachi and ors v Moldova*, No 25198/02, Judgment, 10 February 2009, ¶ 43; *Weber and Saravia v Germany*, No 54934/00, Decision, 29 June 2006, ¶ 95.

[45] *Association for European Integration and Human Rights*, *supra* n. 43, ¶ 75; *Leander*, *supra* n. 43, ¶ 50; *Halford v the United Kingdom*, No 20695/92, Judgment, 25 June 1997, ¶ 49.

[46] *Halford*, *supra* n. 45, ¶ 49; *Association for European Integration and Human Rights*, *supra* n. 44, ¶ 77; *PG and JH v the United Kingdom*, No 44787/98, Judgment, 25 September 2001, ¶ 46.

[47] *Iordachi*, *supra* n. 44, ¶¶ 43-46; cf. *MN and ors v San Marino*, No 28005/12, Judgment, 7 July 2015, ¶ 77.

[48] *Association for European Integration and Human Rights and Ekimdzhiev*, *supra* n. 44, ¶¶ 90-91.

[49] Cf. *ibid.* at ¶ 92-93.

[50] *Kennedy*, *supra* n. 37, ¶¶ 160-170.

[51] *Weber and Saravia*, *supra* n. 44, ¶¶ 26-27, 32, 44, 96-99.

time when the type of communication involved—wireless telephone conversations—accounted for only ten per cent of all telephone communications.[52]

**37.** By contrast, the Court has never found that a scheme requiring the capture and retention of communications data pertaining to *all* communications, whether internal or external and regardless of the existence any individualised suspicion, was necessary in a democratic society and therefore complied with the Convention.[53] Particularly in light of the explosive growth in the use of Internet communication services and technologies and the resulting intrusiveness of such a scheme, as well as the manifest incompatibility of universal, omnipresent, indefinite surveillance with the very notion of a democratic society, the French scheme clearly exceeds what could reasonably be regarded as 'necessary in a democratic society' for the purposes of Article 8 and thus violates the Convention.

**38.** The ruling of the Court's Grand Chamber in *S and Marper v the United Kingdom* supports this view. In that case, the Court held that a Contracting Party's '*blanket and indiscriminate*' powers to retain the biometric information of individuals who had not been convicted of a crime constituted a disproportionate interference with the applicants' right to private life and were not necessary in a democratic society.[54] Central to the Court's reasoning was the absence of any conviction in the applicants' cases, as well as the fact that the law permitted the government to retain the data '*irrespective of the nature or gravity of the offence with which the individual was originally suspected*'.[55] The Court also criticised the law's failure to provide for an '*independent review of the justification for the retention according to defined criteria, including such factors as the seriousness of the offence, previous arrests, the strength of the suspicion against the person and any other special circumstances.*'[56] We submit that the same reasoning applies in this case, and that the data-retention provisions at issue violate Article 8 in requiring non-targeted collection and storage.

**39.** We defer to the claimants as to whether other characteristics of the provisions in question, such as the authorisation, oversight, or access schemes, violate the legality or necessity requirements that Article 8 imposes.

## IV. A majority of other national courts have struck down similar legislation

**40.** Our research suggests that within the EU, most national courts that have considered the issue to date have struck down provisions of national legislation that implemented the Data Retention Directive, as Article R10-13 of the Code of postal and electronic communications was originally intended to do.[57] In doing so, national judges have concluded that the imposition of non-targeted, compulsory data retention violated the rights to privacy and the protection of personal data found in the Charter, the ECHR and the case-law of the ECtHR, and/or their respective national constitutions and fundamental-rights laws.

---

[52] *Ibid.* at ¶¶ 27, 30.

[53] The question of whether a strategic monitoring scheme concerning external Internet communications complied with Article 8 was presented in *Liberty*; as the Court found that the scheme in question was not implemented 'in accordance with the law', it did not reach the issue of whether such a scheme could be 'necessary in a democratic society'. We note, however, that the Court appears to have implicitly demonstrated concern regarding the '*virtually unfettered*' discretion of the Contracting Party's authorities to capture '*very broad classes of communications*'. *Liberty*, *supra* n. 37, ¶ 64.

[54] *S and Marper*, *supra* n. 33, ¶ 125.

[55] *Ibid.* at ¶ 119.

[56] *Ibid.*

[57] See ¶ 8 above and accompanying reference. Exceptions of which we are aware include the case of *Tele2 Sverige AB v Post- och Telestyrelsen*, which the Stockholm Administrative Court of Appeal has referred to the CJEU (see *infra* n. 68), and a case in which the Hungarian Constitutional Court declined to rule on the merits of national data retention legislation due to procedural issues (see Társaság a Szabadságjogokért & Privacy International, 'Suggestions for privacy-related questions to be included in the list of issues on Hungary, Human Rights Committee, 115th Session, October-November 2015', 7 August 2015, pp. 5-6, available at http://tbinternet.ohchr.org/Treaties/CCPR/Shared%20Documents/HUN/INT_CCPR_ICS_HUN_21421_E.pdf).

**41.** Even before the CJEU issued its judgment in *Digital Rights Ireland*, the constitutional or administrative courts of Bulgaria, Cyprus, the Czech Republic, Germany and Romania declared part or all of the relevant national legislation implementing the Data Retention Directive to be unlawful.[58]

**42.** Following the *Digital Rights Ireland* judgment, the courts of Austria[59], Slovenia[60], Belgium[61], Bulgaria[62], the Netherlands[63], Poland[64], Romania[65], Slovakia[66] and the United Kingdom[67] have struck down national laws that had implemented or replicated the Data Retention Directive (or, in the case of Romania and Bulgaria, subsequent amendments to the original implementing laws).

**43.** Whilst the grounds and scope of these judgments vary, many of them appear to have invalidated the national legislation on the basis of its incompatibility with Articles 7 and 8 of the Charter.[68]

**44.** These decisions provide a clear indication that national laws such as those challenged by the claimants do not comply with Member States' obligations under the Charter.

**Conclusion**

**45.** For the foregoing reasons, we support the claimants' submission that the challenged provisions are unlawful as a matter of EU law. We also submit that the provisions are neither 'in accordance with the law' nor 'necessary in a democratic society' for the purposes of Article 8 of the ECHR, and are therefore in breach of the Convention.

---

[58] Franziska Boehm & Mark D. Cole, *Data Retention after the Judgement of the Court of Justice of the European Union*, 30 June 2014, pp. 17-18, available at https://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm-Cole-data_retention-study-print-layout.pdf.

[59] *Ibid.* at p. 62.

[60] *Ibid.*

[61] *In the matters introduced by the Francophone and German-speaking bars*, *supra* n. 33.

[62] 'Bulgaria's Constitutional Court scraps data retention provisions', *Sofia Globe*, 12 March 2015, available at http://sofiaglobe.com/2015/03/12/bulgarias-constitutional-court-scraps-data-retention-provisions/.

[63] Wendy Zeldin, 'Netherlands: Court Strikes Down Data Retention Law', Library of Congress, 23 March 2015, http://www.loc.gov/law/foreign-news/article/netherlands-court-strikes-down-data-retention-law/.

[64] Open Rights Group, 'Data retention in the EU following the CJEU ruling', April 2015, pp. 12-13, https://www.openrightsgroup.org/assets/files/legal/Data_Retention_status_table_updated_April_2015_uploaded_finalwithadditions.pdf.

[65] *Ibid.* at pp. 13-14.

[66] EDRi, 'Slovakia: Mass surveillance of citizens is unconstitutional', 6 May 2015, https://edri.org/slovakia-mass-surveillance-of-citizens-is-unconstitutional/; see also European Information Society Institute, 'The Slovak Constitutional Court cancelled mass surveillance of citizens', undated, http://www.eisionline.org/index.php/en/projekty-m-2/ochrana-sukromia/109-the-slovak-constitutional-court-cancelled-mass-surveillance-of-citizens.

[67] *Davis & Ors, R (on the application of) v Secretary of State for the Home Department & Ors* [2015] EWHC 2092 (Admin) (17 July 2015). This judgment disapplied provisions of the relevant UK data retention law pertaining to access to and use of the retained data, although it did not disapply the provisions permitting the Secretary of State to issue orders requiring the retention of all communications data. We believe the latter finding rests on an incorrect interpretation of EU law and the *Digital Rights Ireland* judgment and note that the case, in which Privacy International has intervened, is now the subject of an appeal. By contrast, the Belgian Constitutional Court appears to have viewed the indiscriminate retention of data as inconsistent with the Charter as interpreted by the CJEU in *Digital Rights Ireland*, even independently of the regime governing access to the data, which the Constitutional Court also found to be contrary to the Charter (*supra* n. 33).

[68] None of these courts considered a reference to the CJEU to be necessary. On 4 May 2015, the Stockholm Administrative Court of Appeal referred the case of *Tele2 Sverige AB v Post- och Telestyrelsen* to the CJEU (Case C-203/15) asking the Court whether blanket data retention without any distinctions, limitations or exceptions is incompatible with Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (commonly known as the ePrivacy Directive), taking account of Articles 7, 8 and 15(1) of the Charter of Fundamental Rights.