Conseil D'Etat
Section du contentieux
Requete N° 393099 : FDN et al. c. Gouvernement

Tierce intervention

Le Centre pour la Démocratie et la Technologie (« CDT »), une organisation à but non lucratif constituée en vertu des lois du District de Columbia aux États-Unis d'Amérique, le 6 décembre 1994 (autorisation n°53006721), et reconnue comme une organisation à but non lucratif en vertu de l'article 501(c)(3) du code des impôts des États-Unis (identification employeur n°52-1905358),
ayant sa son siège au 1634 I Street Northwest, Suite 1100,
Washington, DC, 20006, États-Unis d'Amérique,
représentée par son Président et Directeur Général, Monsieur Nuala O'Connor,

- et -

Privacy International, qui est une organisation à but non lucratif constituée en 1990
en vertu des lois du Royaume-Uni et d'Irlande du Nord, et est un organisme caritatif agréé, enregistré au Royaume-Uni (n° 1147471),
ayant son siège au 62 Britton Street, Londres, EC1M 5UY, Royaume-Uni,
représentée par son Directeur Général, le Dr. Gus Hosein,

demandent par la présente l'autorisation du Conseil d'État de soumettre la tierce intervention suivante.

I. Introduction et sommaire

1. Le Centre pour la Démocratie et la Technologie (« CDT ») et Privacy International ont l'honneur de soumettre cette tierce intervention dans le cadre du recours de FDN et al. contre Gouvernment (Req. n°393099), devant la dixième sous-section de la section du Contentieux du Conseil d'État. Les demandeurs contestent le refus du gouvernement d'abroger l'article R. 10-13 du code des postes et des communications électroniques et le décret n° 2011-219 du 25 février 2011 concernant la conservation et la communication des données permettant l'identification de toute personne ayant contribué à la création de contenu en ligne.

2. CDT est une organisation non-gouvernementale qui promeut les droits et libertés fondamentaux en ligne, et est engagée pour la recherche de solutions prospectives et techniquement solides en réponse aux défis les plus pressants auxquels sont confrontés les utilisateurs de technologies de communications électroniques. Depuis sa constitution il y a plus de 20 ans, CDT a joué un rôle de premier plan dans l'élaboration de politiques, de pratiques et de normes afin de permettre aux individus

de s'approprier avec efficience les technologies en tant qu'intervenants, entrepreneurs ou citoyens engagés. Basée à Washington DC, l'organisation est un organisme caritatif agréé, enregistré aux États-Unis et disposant de bureaux à Bruxelles. CDT soutient activement le développement rigoureux de lois et de normes européennes respectueuses des droits de l'homme dans les domaines de la vie privée et de la liberté d'expression, et défend également la conformité des lois nationales avec le cadre juridique européen en matière de droits de l'homme lorsqu'il y a lieu.
L'organisation est déjà intervenue devant la Cour européenne des droits de l'homme (CEDH) dans un recours concernant l'accès gouvernemental aux données privées (*Szabó et Vissy c. Hongrie*, n°37138/14) et a demandé la permission d'intervenir dans deux recours devant la CEDH concernant les pratiques de surveillance du Royaume-Uni (*Big Brother Watch et autres c. Royaume-Uni*, n°58170/13 ; *Bureau of Investigative Journalism et Ross c. Royaume-Uni*, n°62322/14). En conséquence, CDT considère avoir qualité et intérêt à intervenir dans la présente affaire.

3. Privacy International (PI) a été constituée en 1990 et a été la première organisation à faire campagne à l'échelle internationale sur les questions de vie privée. L'organisation est basée à Londres et est engagée dans la lutte pour le droit à la vie privée à travers le monde, notamment par la promotion de ce droit, la recherche et le recours au contentieux. Elle est un organisme caritatif agréé, enregistré au Royaume-Uni et défend la vision d'un monde où le droit à la vie privée est pleinement protégé et respecté. Privacy International joue un rôle de premier plan en matière de droit à la vie privée et à la liberté d'expression, et défend les lois nationales et régionales qui protègent ces droits. PI a déjà pris part à plusieurs procédures visant à contester des pratiques de surveillance devant les tribunaux britanniques et devant la Cour EDH, et est intervenue dans des recours hongrois et britanniques concernant la conformité de régimes nationaux de conservation de données avec le droit communautaire (*Dalma Dojcsak c. Telenor Magyarország ZRT ; Davis and Watson c. Secretary of State for the Home Department*). Pour ces raisons, Pl a qualité et intérêt à intervenir dans la présente affaire.

4. Nos organisations soumettent ce mémoire pour aider le Conseil d'État à aborder deux problématiques : la conformité des dispositions réglementaires (article R10-13 du code des postes et des communications électroniques et des postes et le décret n° 2011-219 du 25 février 2011) relatives à la conservation de données contestées avec la Charte des droits fondamentaux de l'Union européenne (ci-après « la Charte ») à la lumière des arrêts *Digital Rights Ireland c. Minister for Communications, Marine and Natural Resources et al.* de la Cour de justice de l'Union européenne (« CJUE ») et *Schrems c. Data Protection Commissioner*[1], ainsi que la conformité desdites dispositions avec l'article 8 de la Convention européenne des droits de l'homme (CEDH).

5. Nos conclusions sont que les dispositions contestées ne sont pas conformes à la Charte et sont donc illégales au regard du droit de l'Union européenne (UE), et que la portée, la durée et la nature systématique de la conservation des données qui en découle viole l'article~8 de la CEDH.

1 CJUE, Grande Chambre (G. C.), 8 avril 2014, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources*, C-293/12, ECLI:EU:C:2014:238, (ci-après « *Digital Rights Ireland* ») et CJUE, 6 octobre 2015, *Schrems c. Data Protection Commissioner*, C-362/14, ECLI:EU:C:2015:650.

II. Les dispositions contestées imposant la conservation de données ne sont pas conformes à la Charte des droits fondamentaux de l'Union européenne et sont donc illégales au regard du droit de l'UE

a. Les obligations contestées de conservation de données appliquent le droit de l'UE et doivent se conformer à la Charte des droits fondamentaux de l'Union européenne

6. Conformément à l'article 51, paragraphe 1 de la Charte, la France est tenue de respecter les droits énoncés dans la Charte chaque fois qu'elle applique le droit de l'Union européenne[2]. La jurisprudence de la CJUE suggère que les dispositions nationales visant explicitement à donner effet au droit de l'UE doivent être lues comme entrant « dans le champ d'application~» du droit de l'UE. En ce sens, des dispositions qui pourraient être affectées par des règles spéciales du droit européen peuvent elles aussi être sujettes au droit de l'union[3].

7. Depuis deux décennies, la législation européenne s'est efforcée d'harmoniser le respect par les États membres du droit à la vie privée dans le cadre des communications électroniques et du traitement des données personnelles[4]. Ce faisant, le législateur européen a règlementé de façon extensive le traitement des données personnelles, y compris en imposant aux États membres qu'ils « garantissent [...] la confidentialité des communications effectuées [...] ainsi que la confidentialité des données relatives au trafic y afférentes » en interdisant, *inter alia*, « de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés sauf lorsque cette personne y est légalement autorisée », en application d'exceptions énoncées dans la législation correspondante[5]. Bien que le droit de l'UE sur ces questions permettent aux États membres d'y déroger pour certains motifs limités, de notre point de vue il ne fait aucun doute qu'un État membre agit dans le cadre du droit de l'UE lorsqu'il adopte des lois ou des mesures règlementaires touchant au traitement des données personnelles[6].

8. Concernant l'application de la première des dispositions contestées, l'article R10-13 du code des postes et des communications électroniques, nous observons que le ministère de la Justice a explicitement confirmé que la France a mis en œuvre le droit communautaire lorsqu'elle a adopté le décret n°2006-356 du 24 mars 2006 (qui a créé l'article R10-13) portant sur la conservation des

2 Union Européenne, Charte des droits fondamentaux de l'Union européenne (2000/C 364/01), signée le 7 décembre 2007 (ci-après « la Charte »).

3 CJUE, 6 mars 2014, *Cruciano Siragusa c. Regione Sicilia*, C-206/13, ECLI:EU:C:2014:126, §§ 20-25 ; voir aussi CJUE, G. C., 26 février 2013, *Åklargen c. Åkerberg Fransson*, C-617/10, ECLI:EU:C:2013:105, § 21 (confirmant que « [l]es droits fondamentaux garantis par la Charte devant, par conséquent, être respectés lorsqu'une réglementation nationale entre dans le champ d'application du droit de l'Union, il ne saurait exister de cas de figure qui relèvent ainsi du droit de l'Union sans que lesdits droits fondamentaux trouvent à s'appliquer. » En conséquence, « [l]'applicabilité du droit de l'Union implique celle des droits fondamentaux garantis par la Charte »).

4 Voir par exemple la Directive 95/46 du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ; Voir aussi la Directive 2002/58 du Parlement européen et du Conseil du 12 juillet 2002 relative à la protection de la vie privée dans le secteur des communications électroniques ; Voir CJUE, 7 novembre 2013, *Institut professionnel des agents immobiliers (IPI)*, C-473/12, EU:C:2013:715, point 28.

5 Directive 2002/58, art. 5(1) et 15(1).

6 Voir les motifs de dérogations de l'article 13 de la Directive 95/46. Dans ce sens, voir CJUE, 30 avril 2014, *Robert Pfleger et autres*, C-390/12, ECLI:EU:C:2014:281, points 33 à 36 sur l'obligation de se conformer à la Charte lors de la prise de mesures d'exception.

données de communications électroniques[7].

9. Quant à la seconde des mesures contestées, le décret n°2011-219 du 25 février 2011, celui-ci oblige les hébergeurs à conserver un large éventail de données y compris, par exemple, les données d'abonnés telles que leur nom et adresse postale, ce qui facilite l'identification de chaque individu créant ou contribuant à tout type de contenu en ligne, incluant potentiellement des communications privées[8]. Nous estimons que le traitement réservé à de telles données par la France (y compris en exigeant leur conservation) est directement soumis à la législation spécifique de l'UE relative à la protection des données personnelles, qui porte sur le traitement de « toute information concernant une personne physique identifiée ou identifiable »[9]. Ainsi, le décret entre dans le champ d'application du droit de l'UE[10].

10. En conséquence, nous considérons que les dispositions françaises dont il est question dans cette requête entrent dans le champ d'application du droit communautaire, de telle manière que les dispositions de la Charte s'appliquent. Il en découle que les dispositions de la Charte s'appliquent.

b. Les exigences de conservation de données en cause dans cette affaire représentent des restrictions des droits à la vie privée et à la protection des données personnelles consacrés par la Charte

11. Le Conseil d'État n'est pas sans ignorer que la Charte prévoit que lorsque les États membres transposent le droit de l'UE, ils se doivent de respecter les droits au « respect de [l]a vie privée et familiale, [du] domicile et [des] communications » (article 7) et la protection des données personnelles (article 8)[11]. Les États membres sont uniquement autorisés à imposer des limitations à ces droits si ces restrictions sont conformes aux critères énoncés dans la Charte (voir paragraphe 17 ci-dessous)[12].

12. Dans son arrêt rendu dans deux affaires jointes, connu sous le nom *Digital Rights Ireland*, la CJUE a constaté que « l'obligation imposée [...] aux fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communication de conserver pendant une

---

7 La France a adopté ce décret afin de transposer la Directive 2006/24/CE sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, dite Directive sur la conservation de données ; Voir la question écrite n°54372 de M. Lionel Tardy, 22 avril 2014, disponible à cette adresse : http://questions.assemblee-nationale.fr/q14/14-54372QE.htm. Comme indiqué plus bas, la CJUE a par la suite invalidé la directive sur la conservation des données dans son intégralité en invoquant son incompatibilité avec la Charte ; toutefois, la Cour avait déjà souligné que le législateur de l'Union disposait d'une base juridique valide pour adopter la directive 2006/24/CE (CJUE, 10 février 2009, *Irlande c. Parlement européen et Conseil de l'Union européenne*, C-301/06, ECLI:EU:C:2009:68), ce qui implique à notre sens que l'adoption du décret n°2006-356 du 24 Mars 2006 demeure une mise en œuvre du droit de l'UE, malgré l'invalidation ultérieure de la directive sur le fondement de droits fondamentaux. En outre, comme expliqué au paragraphe 7 ci-dessus, la France applique le droit de l'Union européenne chaque fois qu'elle adopte des lois ou des règlements concernant le traitement des données personnelles.

8 Décret n°2011-219 du 25 février 2011 concernant la conservation et la communication de données permettant l'identification de toutes les personnes qui ont contribué à la création de contenu en ligne, JORF n°0050 du 1er mars 2011, p. 3643.

9 Directive 95/46/CE, art. 2 et 3.

10 Voir *supra* n°3 et le texte qui l'accompagne.

11 Chapitre, *supra* n°2, art. 7, 8 et 51(1).

12 *Ibid*., art. 52(1).

certaine durée », les données nécessaires à l'identification de la source et de la destination d'une communication téléphonique ou par le biais de l'Internet, ainsi que sa date, son heure, sa durée ainsi que le terminal utilisé, constituait une ingérence dans le droit à la vie privée tel que prévu à l'article 7 de la Charte[13].

13. La Cour a également constaté que ces obligations de conservation de données constituaient une ingérence dans le droit à la protection des données personnelles tel que consacré à l'article 8 de la Charte, car elles « prévoi[ent] un traitement des données à caractère personnel »[14].

14. La Cour a utilisé le terme « ingérence » comme synonyme de « limitations » dans le même sens que lorsqu'il est employé dans l'article 52 (1) de la Charte[15]. Elle a caractérisé les ingérences en cause dans ces affaires vis-à-vis du droit à la vie privée et à la protection des données de « particulièrement grave », observant que « la circonstance que la conservation des données et l'utilisation ultérieure de celles-ci sont effectuées sans que l'abonné ou l'utilisateur inscrit en soient informés est susceptible de générer dans l'esprit des personnes concernées, ainsi que l'a relevé M. l'avocat général aux points 52 et 72 de ses conclusions, le sentiment que leur vie privée fait l'objet d'une surveillance constante »[16].

15. Que la collecte et la conservation des données de communication constitue une ingérence dans le droit à la vie privée a été reconnu par bon nombre d'institutions internationales et d'experts en droits de l'homme, y compris le Groupe de travail Article 29, le Haut Commissariat des Nations Unies aux droits de l'homme, le rapporteur spécial des Nations Unies pour la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, et le Commissaire aux droits de l'homme du Conseil de l'Europe[17].

16. Étant donné que les types de données en l'espèce incluent, voire dépassent, les types de données dont la rétention était en cause dans l'arrêt *Digital Rights Ireland*, nous sommes convaincus que les constats ci-dessus appellent la conclusion que les dispositions françaises, dont les demandeurs veulent obtenir l'abrogation, restreignent les droits à la vie privée et la protection des données, consacrés par la Charte[18].

c. Ces restrictions vont au delà du strict nécessaire et violent donc le droit de l'UE

17. Conformément à la Charte, la France peut uniquement limiter les droits qu'elle consacre si les

13 *Digital Rights Ireland*, supra n°1, § 34.
14 *Ibid*., § 36.
15 Voir *ibid*., §§ 38, 39 et 45.
16 *Ibid*., § 37.
17 Groupe de travail Article 29, avis 04/2014, WP 215 sur la surveillance des communications électroniques à des fins de renseignement et de sécurité nationale (disponible à cette adresse : http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_fr.pdf), 819/14/EN, 10 avril 2014 ; Haut-commissariat des Nations unies aux droits de l'homme, *Le droit à la vie privée à l'ère du numérique*, A/HRC/27/37, 30 juin 2014 ; Rapporteur spécial des Nations-Unies sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, 23 septembre 2014, rapport, *La promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste*, A/69/397 ; Commissaire aux droits de l'homme du Conseil de l'Europe, *La prééminence du droit sur l'internet et dans le monde numérique en général*, 2014.
18 Les demandeurs ont indiqué que le décret n°2011-219 du 25 février 2011 impose des obligations de conservation des données sur les services d'hébergement, et a ainsi une portée encore plus large que celle de la directive sur la conservation des données (invalidée par *Digital Rights Ireland*).

restrictions apportées sont « nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui »[19]. Plus précisément, lorsqu'un Etat cherche à restreindre le « droit au respect de la vie privée, la protection de ce droit fondamental exige, selon la jurisprudence constante de la Cour, en tout état de cause, que les dérogations à la protection des données à caractère personnel » satisfassent au plus haut standard du « stricte nécessaire »[20].

18. Dans *Digital Right Ireland*, la CJUE a relevé que la directive 2006/24/CE relative à la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, courramment appelée directive sur la conservation des données, portait atteinte aux droits à la vie privée et à la protection des données d'une manière dépassant le « strict nécessaire » pour lutter contre la criminalité et assurer la sécurité publique[21]. La Cour est parvenue à cette conclusion pour les raisons suivantes :

- i. la Directive « couvr[ait] de manière généralisée toute personne et tous les moyens de communication électronique ainsi que l'ensemble des données relatives au trafic sans qu'aucune différenciation, limitation ni exception soient opérées en fonction de l'objectif de lutte contre les infractions graves »[22] ;
- ii. elle ne prévo[yait] pas d'exceptions pour les « personnes dont les communications sont soumises, selon les règles du droit national, au secret professionnel »[23] ;
- iii. elle « ne requier[ait] aucune relation entre les données dont la conservation [était] prévue et une menace pour la sécurité publique » : en plus de ne pas exiger un quelconque lien, « même indirect ou lointain », entre les personnes affectées et l'infraction grave, elle n'imposait pas de limites temporelles ou géographiques sur les données à conserver[24] ;
- iv. elle négligeait de définir des critères de fond ou de procédure régissant l'accès des autorités nationales compétentes aux données ou limitant le nombre d'autorités qui pourraient obtenir un tel accès[25] ;
- v. elle n'imposait pas que l'autorisation d'accès aux données conservées dépende « [d']un contrôle préalable effectué soit par une juridiction, soit par une entité administrative

19 La Charte, *supra* n°2 art. 52(1).
20 *Digital Rights Ireland*, supra n°1, § 52 (citant *IPI c. Englebert*, *supra* n°3, § 39).
21 *Ibid.*, §§ 41 et 65.
22 *Ibid*., §57 ; Voir aussi CJUE, 6 octobre 2015, *Schrems c. Data Protection Commissioner*, *supra*, §93 (« Ainsi, n'est pas limitée au strict nécessaire une réglementation qui autorise de manière généralisée la conservation de l'intégralité des données à caractère personnel de toutes les personnes dont les données ont été transférées depuis l'Union vers » un pays tiers « sans qu'aucune différenciation, limitation ou exception soit opérée en fonction de l'objectif poursuivi »).
23 *Digital Rights Ireland*, *supra* n°1, § 58.
24 *Ibid*., §§ 58 et 59 ; cf. *Schrems*, *supra* n°22, §93 (indiquant que la législation concernant le stockage des données personnelles doit énoncer « un critère objectif permettant de délimiter l'accès des autorités publiques aux données et leur utilisation ultérieure à des fins précises, strictement restreintes et susceptibles de justifier l'ingérence » qui ont entraîné l'accès et l'utilisation des données).
25 *Digital Rights Ireland*, *supra* n°1, §§ 60 à 62 ; Voir aussi *Schrems*, *supra* n°22, §90 (indiquant que l'accès des autorités aux données personnelles, et leur traitement ultérieur, se doit d'être « strictement nécessaire et proportionné » par rapport à un objectif légitime).

indépendante dont la décision vise à limiter l'accès aux données et leur utilisation à ce qui est strictement nécessaire [...] et [qui] intervient à la suite d'une demande motivée de ces autorités présentée dans le cadre de procédures de prévention, de détection ou de poursuites pénales »[26] ;

- vi. elle n'imposait pas que l'utilisation ultérieure des données soit obligatoirement cantonnée à la prévention, la détection ou l'engagement de poursuites pénales, ou que ces infractions soient obligatoirement d'une gravité suffisante pour justifier l'atteinte grave aux droits fondamentaux en cause[27] ;
- vii. elle ne prévoyait pas d'exigence que la période de conservation « [soit] fondée sur des critères objectifs afin de garantir que celle-ci [soit] limitée au strict nécessaire », ou que des distinctions soient établies à cet égard entre les catégories de données en fonction de leur utilité dans la poursuite d'un but légitime[28] ;
- viii. elle n'établissait pas de garanties suffisantes permettant d'assurer la sécurité des données[29] ;
- ix. elle ne prescrivait pas que les données devaient être irréversiblement détruites à la fin de la période de conservation[30] ; et
- x. elle n'imposait pas que les données soient conservées au sein de l'UE[31].

19. Selon nous, l'inclusion par la Cour de ces critères indique que chacun est un volet des droits applicables consacrés dans la Charte et qu'ainsi, ils sont une condition à remplir pour les institutions de l'UE et les États membres lorsqu'ils mettent en œuvre le droit de l'Union. La jurisprudence antérieure de la Cour suggère qu'en temps normal, elle aurait invalidé chaque disposition pertinente de la directive sur la conservation des données, et que sa décision d'invalider la directive dans son ensemble s'est fondée sur le fait que tout le texte était dévoyé par les failles pointées par la Cour[32]. En d'autres termes, chacune des caractéristiques décrites ci-dessus doit être considérée comme violant la Charte, indépendamment de tout impact qu'elles puissent avoir cumulativement[33].

---

26 *Digital Rights Ireland*, *supra* n°1, § 62 ; Voir aussi *Schrems*, *supra* n°22, § 90 (soulignant la nécessité de « garanties suffisantes permettant de protéger efficacement leurs données [personnelles] contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données »).

27 *Digital Rights Ireland*, *supra* n°1, §§ 60 et 61 ; Voir aussi *Schrems*, *supra* n°22, § 93.

28 *Digital Rights Ireland*, *supra* n°1, §§ 63 et 64 ; Voir aussi *Schrems*, *supra* n°22, § 93 (indiquant que le stockage de données à caractère personnel doit être soumis à des différenciations, des limitations ou des exceptions opérées en fonction de l'objectif poursuivi).

29 *Ibid*., § 66.

30 *Ibid*., § 67.

31 *Ibid*., § 68. En ce qui concerne cette liste des raisons qui ont fondé les conclusions de la Cour, cf. David ANDERSON, *A Question of Trust: Report ofthe Investigatory Powers Review* (non disponible en français), juin 2015, pp. 87-88.

32 Cf. CJUE, G. C., 1 mars 2011, *Association Belge des Consommateurs Test-Achats et autres c. Conseil de Ministres*, C-236/09, ECLI:EU:C:2011:100 (invalidant une disposition spécifique de la directive 2004/113/CE au motif de son incompatibilité avec la Charte).

33 Le Tribunal de district de La Haye aurait jugé que la CJUE se repose sur ces critères du fait de leur nature cumulative (David Anderson, *supra* n. 31, p. 89), et la High Court of England and Wales dans *Davis & autres*, *infra* n. 67, semble avoir fait de même. En revanche, la Cour constitutionnelle belge semble avoir vu ces critères comme indépendants au moins dans une certaine mesure (dans les questions introduites par l'*Ordre des barreaux francophones et germanophone et al*., Ordre n°84/2015 du 11 juin 2015, pp. 33- 34, disponible à cette adresse : http://www.const-court.be/public/f/2015/2015-084f.pdf). Comme noté ici, nous considérons que chacun des critères énoncés par la CJUE

20. L'arrêt *Schrems c. Data Protection Commissioner* de la CJUE fournit une confirmation supplémentaire que les critères énoncés aux points (i) et (iii) à (vii) ci-dessus couvrent tout stockage de données à caractère personnel entrant dans le champ d'application du droit communautaire, et ne sont pas limités au contexte spécifique pour lequel la Cour les a invoqués dans *Digital Rights Ireland*[34].

21. En ce qui concerne la conformité des dispositions françaises en cause dans cette requête avec les exigences de la Charte telles qu'énoncées dans *Digital Rights Ireland*, nous nous en remettons aux demandeurs pour apprécier si le régime d'accès aux données conservées, permis par ces dispositions, répond aux critères énoncés aux points (iv) et (v) ci-dessus. Nous nous en remettons aussi aux demandeurs quant à la question de savoir si les mesures de protection en place pour assurer la sécurité des données (point viii), telles que celles énoncées à l'article 34 de la loi n°78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés, sont suffisantes.

22. Toutefois, nous estimons que l'article R10-13 du code des postes et des communications électroniques prévoit, à minima, les caractéristiques exposées aux points (i) à (iii), (vi), (vii), (ix) et (x) ci-dessus : il couvre toutes les personnes, tous les moyens de communication électronique, et toutes les données de trafic sans faire de distinction fondée sur la légitimité du but poursuivi ; il ne comprend pas d'exceptions pour les personnes dont les communications sont soumises au secret professionnel ; il ne nécessite pas de lien, du type défini par la CJUE, entre les données à conserver et une menace pour la sécurité publique ; il ne prévoit pas que l'utilisation ultérieure des données doit se limiter à la prévention, la détection ou l'engagement de poursuites d'infractions pénales dont la gravité suffit pour rendre l'atteinte à la vie privée proportionnée ; il ne garantit pas que la période de conservation se limite au stricte nécessaire à partir de critères objectifs ; et il ne contient aucune disposition visant à garantir que les données sont stockées au sein de l'UE et sont irréversiblement détruites à la fin de la période de conservation.

23. Le décret n°2011-219 du 25 février 2011 présente les mêmes caractéristiques, à la différence qu'il s'applique à tous les moyens de la « création de contenu en ligne » plutôt qu'à tous les moyens de communication électronique en tant que tels.

24. En somme, ces dispositions présentent plusieurs des caractéristiques prohibées décrites au paragraphe 18 ci-dessus, et constituent pour cette raison des restrictions inacceptables des droits énoncés aux articles 7 et 8 de la Charte ; elles sont donc en violation de la législation européenne. Nous nous en remettons aux demandeurs quant à la question de savoir si d'autres aspects de ces dispositions peuvent aussi violer le droit de l'Union.

III. Les dispositions contestées violent l'article 8 de la Convention européenne des droits de l'homme

dans *Digital Rights Ireland* reflète, individuellement, une exigence de la Charte, et nous estimons que le Conseil d'État doit adopter une telle approche. Voir CEDH, G. C., 4 décembre 2008, *S. et Marper c. Royaume-Uni*, Req. Nos 30562/04 et 30566/04, § 99 (décrivant comme « essentiel[le] » l'existence de règles claires et détaillées régissant la portée et l'application des mesures et imposant un minimum d'exigences concernant, notamment, la durée, le stockage, l'utilisation, l'accès des tiers, les procédures destinées à préserver l'intégrité et la confidentialité des données et les procédures de destruction de celles-ci »). En dépit de la position du Conseil d'État, nous estimons que les dispositions françaises contestées de conservation des données demeurent invalides au moins dans la mesure où elles présentent les caractéristiques énumérées ici (voir §§ 21-23).

34 Voir *supra* nn. 22, 24-28 et le texte qui accompagne.

25. L'article 8 de la CEDH reconnaît à chaque personne dépendant de la juridiction française le droit au respect de sa vie privée et de sa correspondance. L'État ne peut pas restreindre ce droit, sauf si une telle ingérence est « prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire » pour atteindre l'un des objectifs énumérés dans cet article, comme ceux de la sécurité nationale, de la prévention d'atteintes à l'ordre publique ou de prévention des crimes[35].

26. La CEDH a déjà jugé que la collecte et le stockage d'informations liées aux communications téléphoniques, telles que la date et la durée d'une conversation ainsi que le numéro composé, constituent des ingérences dans le droit au respect de la vie privée, même si le contenu de la conversation n'est pas rendu accessible ou analysé[36]. Du fait que la Cour a considéré de manière constante l'usage du téléphone, des e-mails, de la télécopie et des autres formes de communication exécutées grace à des outils technologiques, comme soumis aux garanties du même article 8, cette position doit être présumée comme s'étendant aux informations personnelles transmises ou stockées via Internet[37].

27. La Cour a en outre confirmé que même « le simple fait de mémoriser des données relatives à la vie privée d'un individu constitue une ingérence au sens de l'article 8 », indépendamment de savoir si ou comment les données sont utilisées par la suite, si elles sont « sensibles » ou si l'individu subit des « éventuels inconvénients »[38]. Des informations concernant les activités économiques, professionnelles ou même publiques d'une personne peuvent etre comprises dans le champ de la « vie privée », de sorte que la collecte et le stockage par l'Etat des données relatives à ces activités peuvent constituer une violation de l'article 8[39].

28. Conformément à la jurisprudence de la Cour, même la simple existence d'une législation autorisant ou exigeant la collecte et le stockage équivaut à une atteinte selon les finalités de l'article 8, indépendamment de la façon dont la loi est mise en œuvre dans la pratique ; comme la Cour l'a observé, la « menace de surveillance entravant forcément la liberté de communication entre usagers » de services téléphonique et d'autres services de communication[40].

29. Au vu de cette jurisprudence, nous estimons que les dispositions françaises contestées, par lesquelles l'État mandate la collecte et le stockage systématique des données relatives à la totalité ou la quasi-totalité de l'Internet et des communications téléphoniques, constituent incontestablement une violation de l'article 8.

30. Du fait que les activités visées constituent une ingérence, elles se doivent, conformément au second paragraphe de l'article 8 de la Convention, d'etre « prévue[s] par la loi » et être nécessaires dans une société démocratique afin d'être conformes à l'État de droit[41]. Dans le contexte de la « surveillance secrète » (un terme qui couvre a minima la collecte obligatoire, le stockage, la recherche et l'utilisation des données liées aux correspondances, et, selon nous, la création de contenu en ligne), la Cour a

35 Convention pour la protection des droits de l'homme et des libertés fondamentales (ci-après la « CEDH »), arts. 1 et 8.

36 CEDH, 4ème Sect., 3 avril 2007, *Copland c. Royaume-Uni*, Req. n°62617/00, §§ 43-44; voir aussi CEDH, G. C., 4 mai 2000, *Rotaru c. Roumani*e, Req. n°28341/95, § 46.

37 Voir, par exemple, CEDH, 4ème Sect., 1 juillet 2008, *Liberty et autres c. Royaume-Uni*, Req. n°58243/00, § 56; CEDH, 4ème Sect., 18 mai 2010, *Kennedy c. Royaume-Uni*, Req. n°26839/05, § 118.

38 CEDH, *S. et Marper*, supra n. 33, § 67; CEDH, G. C., 16 février 2000, *Amann c. Suisse*, Req. N°27798/95, §§ 69, 70.

39 CEDH, 1ère Sect., 21 juin 2011, *Shimovolos c. Russie*, Req. N°30194 / 09, § 65; CEDH, 16 décembre 1992, *Niemietz c.Allemagne*, Req. N°13710/88, §§ 29-31.

40 Voir CEDH, plénière, 6 septembre 1978, *Klass et Autres c. Allemagne*, Req. N°5029/71, § 41.

41 CEDH, supra n. 35.

précisé que de telles ingérences sont « caractéristique[s] de l'État policier » et que « le pouvoir de surveiller en secret les citoyens n'est tolérable d'après la Convention que dans la mesure strictement nécessaire à la sauvegarde des institutions démocratiques »[42].

31. La CEDH ne s'est pas encore prononcée quant à la question spécifique de savoir si un régime de conservation de données non-ciblées portant sur la quasi-totalité des communications téléphoniques ou par l'Internet envoyées ou reçues par toute personne relevant de la juridiction d'une Partie contractante peut être considéré comme satisfaisant aux exigences de légalité et de nécessité imposées par le second paragraphe de l'article 8. Toutefois, la jurisprudence de la Cour suggère fortement qu'un tel régime, même s'il poursuit un but légitime, ne peut pas être considéré comme « prévu par la loi » ou proportionné et donc, viole la Convention[43].

32. Concernant les critères de conventionnalité figurant au second paragraphe de l'article 8, nous observons que la Cour exige des Parties contractantes qu'elles imposent des restrictions aux ingérences possibles au droit au respect de la vie privée en droit national, y compris (*inter alia*) « la nature des infractions qui peuvent donner lieu » aux ingérences et «~une définition des catégories de personnes susceptibles d'avoir leurs communications surveillées »[44]. D'une manière générale, « la loi doit user de termes assez clairs pour [...] indiquer [aux citoyens] de manière adéquate en quelles circonstances et sous quelles conditions elle habilite la puissance publique à se livrer à » la surveillance[45]. Ces restrictions sont conçues pour protéger les individus des ingérences « arbitraires » dans leur vie privée[46]. Ainsi, la Cour a constaté des violations de l'article 8 lorsque les lois nationales permettaient aux autorités de surveiller de larges, ou potentiellement larges, catégories de personnes, en particulier des personnes n'ayant pas été impliquées dans des infractions graves[47].

33. En outre, la Cour a indiqué par le passé qu'un programme de surveillance ne peut pas être « conforme à la loi » s'il ne permet pas d'assurer que les personnes qui sont surveillés sont informées de cette surveillance (même *ex post facto*)[48].

34. Nous observons que chacune de ces exigences perdrait toute raison d'être si les Parties contractantes étaient autorisées à adopter des régimes de conservation de données incluant la collecte et le stockage, pour une année, voire plus, de données éminemment sensibles relatives à quasiment toutes les communications envoyées, reçues ou encore émises par tout un chacun au sein de leurs juridictions. Nous en concluons donc que les régimes mis en place par les dispositions françaises en cause dans

---

42 *Klass*, *supra* n. 40, § 42; voir aussi *Rotaru*, supra n. 36, § 47; CEDH, 1ère Sect., 15 janvier 2015, *Dragojević c. Croatie*, Req. N°68955/11, § 84; *Kennedy*, *supra* n. 37, § 153.

43 Conformément à la jurisprudence de la Cour, une atteinte au droit à la vie privée doit être proportionnée à un but légitime afin d'être qualifiable de « nécessaire dans une société démocratique », au sens des objectifs poursuivis par l'article 8, § 2 de la Convention. Voir CEDH, 26 mars 1987, *Leander c. Suède*, Req. N° 9248/81, § 58; *Niemietz*, supra n. 39, § 37; CEDH, 28 janvier 2003, *Peck c. Royaume-Uni*, Req. N°44647/98, § 76.

44 CEDH, 28 juin 2007, *Association pour l'intégration européenne et les droits de l'homme et Ekimdzhiev c. Bulgarie*, Req. N°62540/00, § 76; cf. *Kennedy*, supra n. 37, § 160; CEDH, 4ème Sect., 10 février 2009, *Iordachi et Autres c. Moldova*, Req. N°25198/02, § 43; CEDH, 29 juin 2006, *Weber et Saravia c. Allemagne*, Req. N°54934/00, § 95.

45 *Association pour l'intégration européenne et les droits de l'homme*, supra n. 43, § 75; *Leander, supra* n. 43, § 50; CEDH, 25 juin 1997, *Halford c. Royaume-Uni*, Req. N°20695/92, § 49.

46 *Halford, supra* n. 45, § 49; *Association pour l'intégration européenne et les droits de l'homme*, *supra* n. 44, § 77; CEDH, 3ème Sect., 25 septembre 2001, *PG et JH c. Royaume-Uni*, Req. N°44787/98, § 46.

47 *Iordachi*, *supra* n. 44, §§ 43-46; cf. CEDH, 3ème Sect., 7 juillet 2015, *MN et Autres c. San Marino*, Req. N°28005/12, § 77.

48 *Association pour l'intégration européenne et les droits de l'homme et Ekimdzhiev*, *supra* n. 44, §§ 90-91.

cette affaire ne sont pas « en conformité avec la loi » et violent la Convention[49].

35. Concernant le critère de nécessité prévu au second paragraphe de l'article 8, la Cour a fortement laissé entendre que dans tous les cas, lorsque les communications sont internes (c'est à dire qu'elles ont lieu uniquement entre des personnes au sein de la juridiction de l'Etat contractant), une mesure individuelle est exigée, et la nature et la durée de la surveillance doivent également être limitées en fonction des besoins de l'enquête d'espèce[50].

36. Par ailleurs, alors même que la décision de la quatrième section de la Cour en matière de recevabilité dans l'affaire *Weber et Saravia c. Allemagne* peut être lue comme autorisant certaines formes de « surveillance dite[s] stratégique[s] » lorsque cela concerne des communications externes, nous estimons que la quatrième section semble s'être considérée compétente pour apprécier la surveillance (et la transmission des données de surveillance à d'autres autorités) qui avait été pensée pour être actionnée lors de l'usage de « mots clés » au cours de conversations téléphoniques internationales sans fil. En conséquence ces activités, comme l'entendait la quatrième section, étaient de nature individualisées (ou tout du moins discriminées) et autorisées uniquement dans le cadre de l'instruction et de la prévention de certaines infractions graves[51]. (Nous émettons cette observation sans nous prononcer en faveur de l'interpretation apparente de la quatrième section quant la question de savoir si l'atteinte portée à l'article 8 était justifiée.) De plus, la quatrième section a rendu ses conclusions dans le cadre de l'affaire *Weber et Saravia* à une époque où le type de communication en cause, les conversations téléphoniques sans fil, ne représentaient que dix pour cent de toutes les communications téléphoniques[52].

37. Cependant, la Cour n'a jamais considéré qu'un régime exigeant la collecte et la conservation de données de communications se rapportant à *toutes* les communications, qu'elles soient internes ou externes, et indépendamment de l'établissement de soupçons précis, était nécessaire dans une société démocratique et donc conforme à la Convention[53]. En particulier à la lumière de la croissance exponentielle de l'utilisation de services et de technologies de communication passant par l'Internet et du caractère intrusif résultant d'un tel régime, ainsi que l'incompatibilité manifeste d'une surveillance universelle, omniprésente, et non-spécifique avec la notion même de société démocratique. Le régime français excède largement ce qui pourrait être raisonnablement considéré comme des mesures nécessaires dans une société démocratique au vu des objectifs de l'article 8 et, pour cette raison, viole la Convention.

38. L'arrêt *S. et Marper c. Royaume-Uni* rendu par la Grande Chambre corrobore cette approche. La Cour a jugé dans cette affaire que « le caractère général et indifférencié » des pouvoirs d'une Partie contractante sur la conservation des informations biométriques de personnes physiques n'ayant pas fait l'objet d'une condamnation pénale constituait une atteinte disproportionnée au droit à la vie privée des

---

49 Cf. *ibid*. au § 92-93.

50 *Kennedy, supra* n. 37, 160-170 §§.

51 *Weber et Saravia, supra* n. 44, §§ 26-27, 32, 44, 96-99.

52 *Ibid*. au §§ 27, 30.

53 La question de savoir si un système de veille stratégique des communications Internet à destination ou en provenance de l'étranger est conforme à l'article 8 a été soulevée dans l'arrêt *Liberty*. La Cour a trouvé que le régime en question ne respectait pas les mesures « prévues par la loi », mais ne s'est pas prononcée sur le fait qu'un tel système pourrait être « nécessaire dans une société démocratique ». Nous notons, toutefois, que la Cour semble avoir implicitement démontré sa préoccupation concernant la discrétion « pratiquement illimitée » laissée aux autorités de la Partie contractante pour « intercepter [les communications] de manière très large ». *Liberty*, *supra* n. 37, § 64.

requérants et qu'ils ne sont pas nécessaires dans une société démocratique[54]. Le raisonnement de la Cour se fondait principalement sur l'absence de toute condamnation dans les faits d'espèce, et sur le fait que la loi permettait au gouvernement de conserver les données « quelles que soient la nature et la gravité des infractions dont la personne était à l'origine soupçonnée »[55]. La Cour a également condamné l'incapacité de la loi à assurer un « un contrôle indépendant de la justification de la conservation sur la base de critères précis, tels que la gravité de l'infraction, les arrestations antérieures, la force des soupçons pesant sur la personne ou toute autre circonstance particulière »[56]. Nous estimons que le même raisonnement vaut dans le cas présent, et que les dispositions contestées de conservation de données violent l'article 8 en exigeant une collecte et un stockage non-ciblés.

39. Nous nous en remettons aux demandeurs quant à là question de savoir si d'autres caractéristiques des dispositions contestées, telles que les régimes d'autorisation, de contrôle, ou d'accès, violent les exigences de légalité ou de nécessité découlant de l'article~8.

IV. Une majorité des autres juridictions nationales ont abrogé leurs législations analogues

40. Notre étude tend à démontrer qu'au sein de l'UE, la plupart des tribunaux nationaux ayant examiné la question à ce jour ont abrogé les dispositions législatives nationales qui transposaient la directive sur la conservation des données, comme c'était initialement le cas avec l'article R10-13 du code de postes et communications électroniques[57]. Ce faisant, les juges nationaux ont conclu que la mise en place d'une conservation obligatoire et non-ciblée de données violait les droits à la vie privée et à la protection des données personnelles tels que consacrés dans la Charte, la CEDH et la jurisprudence de la CEDH, et/ou leurs constitutions nationales respectives ainsi que leurs lois relatives aux droits fondamentaux.

41. Même avant que la CJUE ne rende sa décision dans l'affaire *Digital Rights Ireland*, les juridictions constitutionnelles ou administratives de Bulgarie, de Chypre, de la République tchèque, d'Allemagne et de Roumanie déclaraient illégales tout ou partie de leurs législations nationales transposant la directive sur la conservation des données[58].

---

54 *S. et Marper, supra* n. 33, § 125.

55 *Ibid.* à § 119.

56 Ibid.

57 Voir § 8 ci-dessus ainsi que la référence jointe. Des exceptions dont nous avons connaissance comprennent l'affaire *Tele2 Sverige AB c. Post-och Telestyrelsen*, dont le tribunal administratif d'appel de Stockholm a renvoyé à la CJUE (voir *infra* n.68), et une affaire pour laquelle la Cour constitutionnelle hongroise a refusé de se prononcer sur les mérites de la législation nationale de conservation des données ppour des raisons procédurales (voir Társaság aSzabadságjogokért & Privacy International, « Suggestions faites aux questions de confidentialité à inclure dans la liste des questions sur la Hongrie, Comité des droits de l'homme, 115e session, octobre-novembre 2015 », 7 août 2015, pp.5-6, disponible à cette adresse : http: //tbinternet.ohchr.org/Treaties/CCPR/Shared %20Documents/HUN/INT_CCPR_ICS_HUN_21421_E.pdf).

58 Franziska Boehm et Mark D. Cole, La conservation des données après l'arrêt de la Cour de justice de l'Union européenne (Data Retention after the Judgement of the Court of Justice of the European Union), le 30 juin 2014, pp.17-18, disponible à cette adresse (uniquement en anglais) : https://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm-Cole-data_retention-study-print-layout.pdf.

42. Suite à l'arrêt *Digital Rights Ireland* les tribunaux de l'Autriche[59], de la Slovénie[60], de la Belgique[61], de la Bulgarie[62], des Pays-Bas[63], de la Pologne[64], de la Roumanie[65], de la Slovaquie[66] et du Royaume-Uni[67] ont abrogé les lois nationales transposant ou répliquant la directive sur la conservation des données (ou, dans le cas de la Roumanie et de la Bulgarie, les amendements subséquents apportés aux lois d'application originales).

43. Tout en prenant acte du fait que les motifs et la portée de ces arrêts varient, beaucoup d'entre eux ont justemment invalidé la législation nationale sur la base de son incompatibilité avec les articles 7 et 8 de la Charte[68].

44. Ces décisions donnent une indication claire que des mesures nationales telles que celles contestées par les demandeurs ne sont pas conformes avec les obligations des États membres en vertu de la Charte.

---

59 *Ibid*. p. 62.

60 Ibid.

61 *Dans les questions introduites par les barreaux francophones et germanophones*, *supra* n. 33.

62 « *La Cour constitutionnelle bulgare met au rebus les dispositions de conservation des données* » (*Bulgaria's Constitutional Court scraps data retention provisions*), Sofia Globe, le 12 mars 2015, disponible à cette adresse (uniquement en anglais) : http://sofiaglobe.com/2015/03/12/bulgarias-constitutional-court-scraps-data-retention-provisions/.

63 Wendy Zeldin, « Pays-Bas : la Cour abandonne la loi sur la conservation des données » (Netherlands: Court Strikes Down Data Retention Law), Bibliothèque du Congrès, le 23 mars 2015, disponible à cette adresse (uniquement en anglais) : http://www.loc.gov/law/foreign-news/article/netherlands-court-strikes-down-data-retention-law/.

64 Open Rights Group, « La conservation des données dans l'UE à la suite de la décision de la CJUE », avril 2015, pp. 12-13, disponible à cette adresse (uniquement en anglais) https://www.openrightsgroup.org/assets/files/legal/Data_Retention_status_table_updated_April_2015_uploaded_finalwithadditions.pdf.

65 *Ibid*. aux pp. 13-14.

66 EDRI, « Slovaquie : La surveillance de masse des citoyens est inconstitutionnelle » (Slovakia: Mass surveillance of citizens is unconstitutional), 6 mai 2015, disponible à cette adresse (uniquement en anglais) https://edri.org/slovakia-mass-surveillance-of-citizens-is-unconstitutional/ ; Voir aussi le European Information Society Institute, « la Cour constitutionnelle slovaque a annulé la surveillance de masse des citoyens » (The Slovak Constitutional Court cancelled mass surveillance of citizens), non daté, disponible à cette adresse (uniquement en anglais) http://www.eisionline.org/index.php/en/projekty-m-2/ochrana-sukromia/109-the-slovak-constitutional-court-cancelled-mass-surveillance-of-citizens.

67 Royaume-Uni, Haute Court de Justice, 17 juillet 2015, *Davis et Autres, R. (on the application of) c. Secretary of State for the Home Department & Autres*, 2092. Cette décision a permis l'annulation de dispositions de la législation britannique en matière de conservation des données relatives à l'accès et à l'exploitation des données conservées, même si elle n'a pas écarté les dispositions permettant au secrétaire d'État de rédiger des arrêtés exigeant la conservation de toutes les données de communication. Nous considérons que cette observation découle d'une interprétation incorrecte de la législation européenne et de l'arrêt *Digital Rights Ireland* et notons que l'affaire, dans laquelle Privacy International est intervenue, fait maintenant l'objet d'un appel. En revanche, la Cour constitutionnelle belge semble avoir apprécié la conservation indiscriminée de données comme étant en contravention avec la Charte telle qu'interprétée par la CJUE dans *Digital Rights Ireland*, même indépendamment du régime régissant l'accès aux données, que la Cour constitutionnelle a également jugé contraire à la Charte (*supra* n. 33).

68 Aucune de ces cours n'a jugé nécessaire de renvoyer ces affaires devant la CJUE. Le 4 mai 2015, la Cour administrative d'appel de Stockholm a renvoyé l'affaire *Tele2 Sverige AB c. Post-och Telestyrelsen* devant la CJUE (Aff.C-203/15 : http://curia.europa.eu) en lui demandant de se positionner sur la compatibilité d'une conservation générale des données sans distinction restriction ou exception avec la Directive 2002/58/CE, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (communément appelée directive ePrivacy), et des articles 7, 8 et 15 (1) de la Charte des droits fondamentaux.

45. Pour les raisons exposées précédemment nous soutenons la position des demandeurs selon laquelle les dispositions contestées sont illégales au regard du droit de l'Union européenne. Nous soutenons également que les dispositions visées ne sont ni conformes à la loi ni nécessaires dans une société démocratique au sens de l'article 8 de la CEDH, et qu'elles sont donc en violation de la Convention.