Conseil d'État
Section du contentieux

Requête introductive d'instance

introduite

PAR

1. **French Data Network (Réseau de données français)**, dite FDN.
   Association régie par la loi du 1er juillet 1901 établie 16 rue de Cachy, 80090 Amiens, enregistrée en préfecture de la Somme sous le numéro W751107563, opérateur déclaré auprès de l'ARCEP sous la référence 07/1149, prise en la personne de son président M. Fabien Sirjean.
   Tél. : 06 36 18 91 00
   Mail : `president@fdn.fr` / `buro@fdn.fr`
2. **La Quadrature du Net**
   Association régie par la loi du 1er juillet 1901 établie au 60 rue des Orteaux 75019, Paris, enregistrée en préfecture de police de Paris sous le numéro W751218406, prise en la personne de son président M. Philippe Aigrain.
   Tél. : 06 73 60 88 43
   Mail : `contact@laquadrature.net`
3. **Fédération des fournisseurs d'accès à Internet associatifs**, dite Fédération FDN (FFDN).
   Fédération régie par la loi du 1er juillet 1901 établie 16 rue de Cachy, 80090 Amiens, enregistrée en préfecture de la Somme sous le numéro W751210904, regroupant 27 fournisseurs d'accès associatifs français, déclarés auprès de l'ARCEP, et un fournisseur d'accès associatif belge déclaré auprès du régulateur, prise en la personne de son président M. Benjamin Bayart.
   Tél. : 06 60 24 24 94
   Mail : `contact@ffdn.org`

CONTRE

Le refus implicite 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 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne, JORF n° 50 du 1er mars 2011, p. 3643.

0. Table des matières

1. FAITS

1.1. Procédure

Premièrement,

L'article L. 34-1, II, alinéa premier, du code des postes et des communications électroniques (CPCE) dispose que :

> *« Les opérateurs de communications électroniques, et notamment les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, effacent ou rendent anonyme toute donnée relative au trafic, sous réserve des dispositions des III, IV, V et VI. »*

Par dérogation à cette disposition, le III de ce même article dispose que :

> *« Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales ou d'un manquement à l'obligation définie à l'article L. 336-3 du code de la propriété intellectuelle ou pour les besoins de la prévention des atteintes aux systèmes de traitement automatisé de données prévues et réprimées par les articles 323-1 à 323-3-1 du code pénal, et dans le seul but de permettre, en tant que de besoin, la mise à disposition de l'autorité judiciaire ou de la haute autorité mentionnée à l'article L. 331-12 du code de la propriété intellectuelle ou de l'autorité nationale de sécurité des systèmes d'information mentionnée à l'article L. 2321-1 du code de la défense, il peut être différé pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques. Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, détermine, dans les limites fixées par le VI, ces catégories de données et la durée de leur conservation, selon l'activité des opérateurs et la nature des communications ainsi que les modalités de compensation, le cas échéant, des surcoûts identifiables et spécifiques des prestations assurées à ce titre, à la demande de l'Etat, par les opérateurs. »*

Le décret visé par cette dernière disposition est le décret n° 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques, créant l'article R. 10-13 du CPCE.

Le 6 mai 2015, les associations requérantes ont demandé au gouvernement d'abroger cet article R. 10-13 du CPCE comme étant contraire à la Charte des droits fondamentaux de l'Union européenne (Charte de l'UE) et à la directive 2002/58/CE de l'Union

européenne (directive 2002/58) [1] . Le 6 juillet 2015, tacitement, le Gouvernement a refusé de l'abroger.

Secondement,

L'article 6, II, alinéa premier, de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) dispose que :

> *« Les personnes mentionnées aux 1 et 2 du I détiennent et conservent les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires. »*

Le quatrième alinéa de ce même article 6, II, dispose que :

> *« Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, définit les données mentionnées au premier alinéa et détermine la durée et les modalités de leur conservation. »*

Le décret visé par cette dernière disposition est le décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne.

Le 6 mai 2015, les associations requérantes ont demandé au gouvernement d'abroger ce décret n° 2011-219 comme étant contraire à la Charte de l'UE et à la directive 2002/58/CE. Le 6 juillet 2015, tacitement, le Gouvernement a refusé de l'abroger.

1.2. Contexte du recours - Changement de circonstances

Dans les semaines qui suivirent les attentats du World Trade Center en septembre 2001, le Royaume-Uni, la France et l'Italie se saisirent de propositions visant à la conservation généralisée des données de connexion. Ainsi, le Parlement français adoptait la loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne prévoyant l'obligation pour les opérateurs de télécommunications de conserver pour une durée maximale d'un an « certaines catégories de données techniques » dans le but de permettre la mise à disposition d'informations pour l'autorité judiciaire (article 29 de la loi précitée instituant un article L. 32-3-1 dans le CPCE, devenu L. 34-1).

Après les attentats de Madrid en mars 2004 et de Londres en juillet 2005, la Commission européenne fit, le 21 septembre 2005, une proposition de directive visant à généraliser ce dispositif de *"data retention"*. Six mois plus tard, la directive n° 2006/24/CE du 15 mars 2006 imposait le principe de conservation généralisée des données de connexion à l'ensemble des États membres de l'Union, avec une durée de conservation allant de six mois à deux ans.

1. Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), JOUE L 201 du 31 juillet 2002, pp. 37 et s.

À l'époque, les critiques dénonçant l'incompatibilité de ces dispositions avec le respect des droits fondamentaux furent nombreuses. Et, justement, plusieurs lois de transposition nationales furent déclarées inconstitutionnelles, les juges nationaux estimant que ces dispositions emportaient une ingérence disproportionnée dans la vie privée et la liberté de communication de leurs citoyens. Tel fut le cas de la Roumanie (2009), de l'Allemagne (2010), de la Bulgarie (2010), de Chypre (2011) et de la République Tchèque (2011).

Le 8 avril 2014, en réponse aux questions préjudicielles posées dans le cadre de deux recours mettant en cause la validité des lois irlandaise et autrichienne de transposition de la directive 2006/24/CE, la grande chambre de la Cour de justice de l'Union européenne (CJUE) jugeait dans l'arrêt *Digital Rights* que ladite directive était invalide car contraire à la Charte des droits fondamentaux de l'Union européenne.

Par cet arrêt, la Cour a rejeté sans équivoque le principe d'une collecte généralisée des données relatives à des personnes pour lesquelles il n'existe, dit la Cour, « aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec des infractions graves » (§ 58). Cette décision produit depuis une véritable « onde de choc », entraînant de multiples décisions des juridictions de différents États membres invalidant à leur tour les dispositions nationales en la matière.

Alors que la France fut l'une des instigatrices de la généralisation de cette obligation de conservation indifférenciée des données de connexion à l'ensemble de l'Union européenne, ce sont les lois françaises en la matière qui sont remises en cause par le présent recours, dans l'espoir de les voir évincées et, *in fine*, abrogées par le législateur.

En suivant la voie ouverte par la Cour de justice de l'Union européenne, le Conseil d'État doit permettre à la France de retrouver la voie d'une conciliation équilibrée entre la protection des droits au respect de la vie privée et de la liberté de communication d'une part, et la prévention et la poursuite des infractions d'autre part, afin de préserver l'État de droit des dérives amenant à la surveillance généralisée de la population.

À cette fin, les associations requérantes contestent la validité du refus du Gouvernement d'abroger l'article R. 10-13 du CPCE et le décret n° 2011-219 en ce que ceux-ci, principalement, appliquent les articles 6, II, de la LCEN et L. 34-1, III, du CPCE qui établissent chacun un régime de conservation généralisée des données de connexions contraire à la Charte de l'UE et à la directive 2002/58/CE.

2. DISCUSSION - Inconventionnalité du régime de conservation généralisée et indifférenciée des « données techniques »

La Charte de l'UE, en son article 52, et la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales (CEDH), en ses articles 8 et 10, exigent que toute ingérence au droit au respect de la vie privée et à la liberté d'expression soit prévue par la loi, poursuive un objectif d'intérêt général et soit strictement nécessaire à la poursuite de cet objectif.

Par son arrêt *Digital Rights Ireland* du 8 avril 2014, la CJUE a établi le principe que tout régime de conservation généralisée des « données techniques », en ce qu'il constitue une ingérence indiscriminée dans ces droits et libertés de l'ensemble de citoyens, ne peut en aucun cas être strictement nécessaire à la poursuite d'aucun objectif, et viole ainsi systématiquement la Charte de l'UE. **Cette décision crée un changement de circonstances fondamental induisant nécessairement l'illégalité des dispositions réglementaires attaquées.**

Compte tenu du fait que les articles 6, II, de la LCEN et L. 34-1 du CPCE établissent un tel régime, le Gouvernement a violé cette Charte en refusant d'abroger les décrets d'application de ces dispositions, et ce bien que l'ampleur de l'obligation de conservation imposée (section 2.1) et l'impossible limitation d'une telle conservation au strict nécessaire l'y obligaient (section 2.2 page 8).

2.1. L'ingérence massive dans les droits fondamentaux

En droit,

L'article 3 de la directive 2006/24/CE, déclarée contraire à la Charte de l'UE par la CJUE dans son arrêt *Digital Rights*, disposait que :

> *« les États membres prennent les mesures nécessaires pour que les données visées à l'article 5 de la présente directive soient conservées, conformément aux dispositions de cette dernière, dans la mesure où elles sont générées ou traitées dans le cadre de la*

fourniture des services de communication concernés par des fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications. »

Les États membres devaient ainsi prévoir des obligations de conservation s'imposant aux personnes exploitant des réseaux de communications électroniques ou fournissant des services de communications électroniques accessibles au public (article 1er de la directive 2006/24/CE).

2.1.0.1. L'étendue des acteurs concernés

Afin de déterminer le champ de ces obligations, il convient notamment de se référer à l'article 2 de la directive « cadre » 2002/21/CE du 7 mars 2002, à la jurisprudence venant préciser la notion de service de communications électroniques [1] ainsi qu'au considérant 10 du préambule de la directive 2002/21/CE.

En effet, il ressort de la lecture du considérant 10 de la directive 2002/21/CE que la fourniture de services de communications électroniques englobe également, outre les opérateurs télécoms classiques, la fourniture de services de courriers électroniques puisqu'il dispose que « les services de téléphonie vocale et de transmission de courrier électronique sont couverts par la présente directive ». De même, la directive est susceptible de s'appliquer à des services fournis en ligne tels que les services dits « de voix sur IP » ou encore « VoIP » (tels que certains services fournis par l'entreprise Skype) puisque l'Autorité de régulation des communications électroniques et des postes a qualifié certains de ces services de services de communications électroniques [2].

Les catégories d'acteurs concernés par ces obligations de conservation sont donc très nombreuses.

2.1.0.2. L'étendue des données concernées

La conservation à laquelle la directive 2006/24/CE soumettait ces acteurs concernait toutes les données, définies à l'article 5 de cette directive [3], qui permettaient de connaître

1. Voir par exemple CJUE, 30 avril 2014, C-475/12, *UPC c. Nemzeti Média*, point 43, au sujet de la notion de service de communications électroniques :

   « [...] il y a lieu de relever que la circonstance que la transmission du signal a lieu par le truchement d'une infrastructure qui n'appartient pas à UPC est sans pertinence pour la qualification de la nature du service. En effet, seul importe à cet égard le fait qu'UPC est responsable envers les utilisateurs finals de la transmission du signal qui garantit à ces derniers la fourniture du service auquel ils se sont abonnés. »

2. Voir notamment : ARCEP, Skype refuse de se déclarer en tant qu'opérateur, Arcep.fr, 12 mars 2013.

3. Cet article 5 vise :

   « a) les données nécessaires pour retrouver et identifier la source d'une communication [...]

   « b) les données nécessaires pour identifier la destination d'une communication

   « c) les données nécessaires pour déterminer la date, l'heure et la durée d'une communication

l'auteur, le destinataire et la date de toute communication émise par n'importe quel citoyen — rendant cette conservation *généralisée et indifférenciée*.

Dans son arrêt *Digital Rights*, la CJUE a ainsi caractérisé l'ingérence permise par un tel régime de conservation :

> *« 56. Quant à la question de savoir si l'ingérence que comporte la directive 2006/24 est limitée au strict nécessaire, il convient de relever que cette directive impose, conformément à son article 3 lu en combinaison avec son article 5, paragraphe 1, la conservation de toutes les données relatives au trafic concernant la téléphonie fixe, la téléphonie mobile, l'accès à l'internet, le courrier électronique par Internet ainsi que la téléphonie par l'internet. Ainsi, elle vise tous les moyens de communication électronique dont l'utilisation est très répandue et d'une importance croissante dans la vie quotidienne de chacun. En outre, conformément à son article 3, ladite directive couvre tous les abonnés et utilisateurs inscrits. Elle comporte donc* **une ingérence dans les droits fondamentaux de la quasi-totalité de la population européenne***. »*

En l'espèce,

Les dispositions législatives françaises établissent un régime de conservation généralisée similaire et comportent dès lors une même ingérence dans les droits fondamentaux de la quasi-totalité de la population.

En effet, premièrement, l'article L. 34-1, III, du CPCE dispose qu'« il peut être différé [par décret] pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques ». Cet article établit une obligation de conservation imposée aux « opérateurs » — autrement contraints par ce même article d'effacer ou de rendre anonymes ces données immédiatement.

La notion d'« opérateur » est définie à l'article L. 32 du CPCE pour couvrir les mêmes personnes que visait l'obligation de conservation de la directive 2006/24/CE : celles exploitant un réseau de communications [4] et celles assurant pour le public la transmission, l'émission ou la réception de signaux sur ces réseaux [5], à l'exclusion de celles hébergeant ou éditant des contenus accessibles au public [6].

Les données concernées par cette obligation sont toutes celles qui, correspondant aux catégories techniques définies par décret, sont traitées par les opérateurs et concernent n'importe quel citoyen. L'article L. 34-1, VI, précise que « les données conservées [...]

« d) les données nécessaires pour déterminer le type de communication

« e) les données nécessaires pour identifier le matériel de communication des utilisateurs ou ce qui est censé être leur matériel ».

4. L'article L. 32, 15° du CPCE définit notamment comme opérateur toute personne « exploitant un réseau de communications électroniques ouvert au public ».

5. L'article L. 32, 15° du CPCE, définit notamment comme opérateur toute personne « fournissant au public un service de communications électroniques », ces services étant définis au 6° comme « les prestations consistant entièrement ou principalement en la fourniture de communications électroniques », ces communications étant définies au 1° comme étant « les émissions, transmissions ou réceptions de signes, de signaux, d'écrits, d'images ou de sons, par voie électromagnétique ».

6. Le 6° de l'article L. 32 précise que « ne sont pas visés les services consistant à éditer ou à distribuer des services de communication au public par voie électronique », ces communications étant définies à l'article 2 de la loi n° 86-1067 du 30 septembre 1986 comme « toute mise à disposition du public ou de catégories de public, par un procédé de communication électronique, de signes, de signaux, d'écrits, d'images, de sons ou de messages de toute nature qui n'ont pas le caractère d'une correspondance privée. »

portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation des équipements terminaux. » et recouvrent donc les mêmes données que celles concernées par la directive 2006/24/CE.

Ainsi, le régime de conservation établi par l'article L. 34-1 du CPCE est identique à celui qu'avait établi la directive 2006/24/CE et, dès lors, l'ingérence qu'il comporte dans les droits et libertés des citoyens est identique et de la même ampleur que celle caractérisée par la CJUE concernant cette directive.

Ensuite, secondement, l'article 6, II, de la LCEN dispose que « les personnes mentionnées aux 1 et 2 du I détiennent et conservent les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires ».

Cette obligation de conservation est mise à la charge des fournisseurs d'accès à Internet [7] — qui sont aussi des opérateurs et étaient donc visés par la directive 2006/24/CE — et des hébergeurs de contenus accessibles au public [8] — qui ne sont pas des opérateurs et étaient expressément exclus du champ de la directive. Les données visées par cette obligation concernent, tout comme celles visées par l'obligation établie par la directive de 2006, n'importe quel citoyen et permettent de l'identifier.

Dès lors, le régime de conservation établi par l'article 6, II, de la LCEN recouvre et dépasse celui qu'avait établi la directive 2006/24/CE. L'ingérence qu'il autorise dans les droits et libertés des citoyens est donc plus importante que celle caractérisée par la CJUE concernant cette directive, en ce qu'il impose aux hébergeurs de conserver les données permettant notamment d'identifier toute personne contribuant à la création d'un contenu.

2.2. L'impossible limitation au strict nécessaire

En droit,

L'article 8, 2, de la Convention européenne des droits de l'homme (Conv. EDH) déclare que :

> *« Il ne peut y avoir ingérence d'une autorité publique dans l'exercice [du droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance] que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. »*

L'article 10, paragraphe 2, de la Convention EDH limite pareillement les restrictions à l'exercice des libertés d'expression, d'opinion et de recevoir ou de communiquer des informations ou des idées.

7. « Les personnes mentionnées [au 1] du I » de l'article 6 de la LCEN sont celles « dont l'activité est d'offrir un accès à des services de communication au public ».

8. « Les personnes mentionnées [au 2] du I » de l'article 6 de la LCEN sont celles « qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services ».

La Cour EDH précise que :

« 101. Une ingérence est considérée comme « nécessaire dans une société démocratique » pour atteindre un but légitime si elle répond à un « besoin social impérieux » et, en particulier, si elle est proportionnée au but légitime poursuivi et si les motifs invoqués par les autorités nationales pour la justifier apparaissent « pertinents et suffisants ». [...]

« 102. Il faut reconnaître à cet égard une certaine marge d'appréciation aux autorités nationales compétentes. Son étendue est variable et dépend d'un certain nombre de facteurs, dont la nature du droit en cause garanti par la Convention, son importance pour la personne concernée, la nature de l'ingérence et la finalité de celle-ci. Cette marge est d'autant plus restreinte que le droit en cause est important pour garantir à l'individu la jouissance effective des droits fondamentaux ou d'ordre « intime » qui lui sont reconnus [...] Lorsqu'un aspect particulièrement important de l'existence ou de l'identité d'un individu se trouve en jeu, la marge d'appréciation laissée à l'Etat est restreinte [...]

« 103. La protection des données à caractère personnel joue un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale consacré par l'article 8 de la Convention. La législation interne doit donc ménager des garanties appropriées pour empêcher toute utilisation de données à caractère personnel qui ne serait pas conforme aux garanties prévues dans cet article [...] La nécessité de disposer de telles garanties se fait d'autant plus sentir lorsqu'il s'agit de protéger les données à caractère personnel soumises à un traitement automatique, en particulier lorsque ces données sont utilisées à des fins policières. ***Le droit interne doit notamment assurer que ces données sont pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées****, et qu'elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées [...] »*

(Cour EDH, g^{de} ch. du 4 décembre 2008, affaire Marper c. Royaume-Uni, n^{os} 30562/04 et 30566/04, § 102 et 103)

De même, l'article 52, paragraphe 1, de la Charte de l'UE déclare que :

« Toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles 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. »

La CJUE précise que, pour être conformes à la Charte, il faut que ces limitations soient « aptes à réaliser les objectifs légitimes poursuivis par la réglementation en cause et ne dépassent pas les limites de ce qui est approprié et nécessaire à la réalisation de ces objectifs. » [9]

De plus, la CJUE précise qu'une limitation doit, pour être conforme à la Charte, être « strictement nécessaire » à l'objectif qu'elle poursuit « en fonction d'un certain nombre d'éléments, parmi lesquels figurent, notamment, le domaine concerné, la nature du droit en cause garanti par la Charte, la nature et la gravité de l'ingérence ainsi que la finalité de celle-ci » et que, ainsi « **s'agissant du droit au respect de la vie privée**, la protection de ce droit fondamental exige, selon la jurisprudence constante de

9. Voir, en ce sens, arrêts Afton Chemical, C-343/09, EU:C:2010:419, point 45 ; Volker und Markus Schecke et Eifert, EU:C:2010:662, point 74 ; Nelson e.a., C-581/10 et C-629/10, EU:C:2012:657, point 71 ; Sky Österreich, C-283/11, EU:C:2013:28, point 50, ainsi que Schaible, C-101/12, EU:C:2013:661, point 29

la Cour, en tout état de cause, que les dérogations à la protection des données à caractère personnel et **les limitations de celle-ci doivent s'opérer dans les limites du strict nécessaire** » [10].

Sur ces fondements, dans son arrêt *Digital Rights*, la CJUE a dégagé un principe selon lequel **rendre obligatoire la conservation de données à caractère personnel concernant la majorité de la population ne peut être strictement nécessaire à la poursuite d'aucun objectif**.

En effet, lors de son examen de la stricte nécessité de l'ingérence prévue par la directive 2006/24/CE, la CJUE a dénoncé avec une insistance singulière la disproportion entre, d'une part, les données dont la conservation était imposée par la directive et, d'autre part, les données dont l'accès par l'autorité publique était nécessaire à la poursuite de l'objectif annonçé par cette directive — la lutte contre les infractions graves.

> *« 57. À cet égard, il importe de constater, en premier lieu, que la directive 2006/24* ***couvre 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****. »*
>
> *« 58. En effet, d'une part, la directive 2006/24* ***concerne de manière globale l'ensemble des personnes faisant usage de services de communications électroniques****, sans toutefois que les personnes dont les données sont conservées se trouvent, même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales. Elle* ***s'applique donc même à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec des infractions graves****. En outre, elle ne prévoit aucune exception, de sorte qu'elle s'applique même à des personnes dont les communications sont soumises, selon les règles du droit national, au secret professionnel. »*
>
> *« 59. D'autre part, tout en visant à contribuer à la lutte contre la criminalité grave, ladite directive ne requiert* ***aucune relation entre les données dont la conservation est prévue et une menace pour la sécurité publique*** *et, notamment, elle n'est pas limitée à une conservation portant soit sur des données afférentes à une période temporelle et/ou une zone géographique déterminée et/ou sur un cercle de personnes données susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave, soit sur des personnes qui pourraient, pour d'autres motifs, contribuer, par la conservation de leurs données, à la prévention, à la détection ou à la poursuite d'infractions graves. »*

Du constat de cette disproportion et de l'ingérence réalisée dans les droits protégés, la CJUE a établi « que cette directive comporte une ingérence dans ces droits fondamentaux d'une vaste ampleur et d'une gravité particulière dans l'ordre juridique de l'Union **sans qu'une telle ingérence soit précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au strict nécessaire**. » (point 65) et, partant, que « le législateur de l'Union a excédé les limites qu'impose le respect du principe de proportionnalité au regard des articles 7, 8 et 52, paragraphe 1, de la Charte » (point 69).

Il ressort ainsi que le caractère strictement nécessaire d'une obligation de conserver des données à caractère personnel dépend de la différence entre, d'une part, les données devant être conservées et, d'autre part, les données dont l'accès est nécessaire à la poursuite de

10. Arrêts Digital Rights précité, point 52 ; IPI, C-473/12, EU:C:2013:715, point 39

l'objectif visé. Ainsi, dès lors que cette différence est absolue — que les données conservées concernent la quasi-totalité de la population —, telle obligation ne peut jamais être strictement nécessaire à la poursuite d'aucun objectif.

En l'espèce,

Tel qu'établi plus tôt (voir section 2.1 page 5), les articles 6, II, de la LCEN et L. 34-1 du CPCE rendent obligatoire la conservation de données à caractère personnel concernant la quasi-totalité de la population. Dès lors, ils réalisent une ingérence dans les droits au respect de la vie privée et à la protection des données à caractère personnel qui ne peut être strictement nécessaire à la poursuite d'aucun objectif.

En conclusion,

Les articles 6, II, de la LCEN et L. 34-1 du CPCE doivent être déclarés contraires à la Charte de l'UE. Partant, le refus du Gouvernement d'annuler le décret n° 2011-219 et l'article R. 10-13 du CPCE pris en leur application doit être annulé.

Subsidiairement,

En considérant que le principe établi par la CJUE dans son arrêt *Digital Rights* est limité par l'objectif poursuivi par la directive alors examinée — que ce principe dispose seulement que rendre obligatoire la conservation de données à caractère personnel concernant la majorité de la population ne peut être strictement nécessaire à la lutte contre des infractions graves —, les dispositions légales françaises visées n'en seraient pas moins contraires à la Charte de l'UE.

En effet, premièrement, les objectifs poursuivis par l'obligation de conservation prévue à l'article L. 34-1 du CPCE ne peuvent que conduire à la même conclusion que celle donnée par la CJUE, étant nettement moins « nécessaires dans une société démocratique » que la lutte contre les infractions graves. Définis au III de cet article, ces objectifs comprennent « les besoins de la recherche, de la constatation et de la poursuite des infractions pénales », et non pas des seules infractions graves, « les besoins de la recherche, de la constatation et de la poursuite [...] d'un manquement à l'obligation définie à l'article L. 336-3 du code de la propriété intellectuelle [11] » et « les besoins de la prévention des atteintes aux systèmes de traitement automatisé de données prévues et réprimées par les articles 323-1 à 323-3-1 du code pénal ».

Ensuite, secondement, l'article 6, II, de la LCEN prévoit une obligation de conservation généralisée sans indiquer d'objectif précis. L'ingérence qu'il permet ne peut dès lors être strictement nécessaire à la poursuite de l'objectif qu'il poursuit — n'en poursuivant aucun — et étant dès lors manifestement contraire au principe de proportionnalité.

Dès lors, les articles 6, II, de la LCEN et L. 34-1 du CPCE doivent être déclarés contraires à la Charte de l'UE. Partant, le refus du Gouvernement d'annuler le décret n° 2011-219 et l'article R. 10-13 du CPCE pris en leur application doit être annulé.

11. Article L. 336-3 du code de la propriété intellectuelle :

« La personne titulaire de l'accès à des services de communication au public en ligne a l'obligation de veiller à ce que cet accès ne fasse pas l'objet d'une utilisation à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits prévus aux livres Ier et II lorsqu'elle est requise. »

Par ces motifs, les exposants concluent à ce que le Conseil d'État :

1. Annule la décision attaquée avec toutes conséquences de droit ;

2. Enjoigne à l'administration d'abroger le décret n° 2011-219 du 25 février 2011 et l'article R. 10-13 du code des postes et communications électroniques ;

3. Mette à la charge de l'État le versement de la somme de 1024 € sur le fondement de l'article L. 761-1 du code de justice administrative.

Le 31 août 2015, à Paris

Pour l'association
French Data Network,
le Président,
Fabien Sirjean

Pour l'association
La Quadrature du Net,
le Président,
Philippe Aigrain

Pour la
Fédération des fournisseurs d'accès à Internet associatif,
le Président,
Benjamin Bayart