Conseil d'État
Section du contentieux
N° 393099

Mémoire complémentaire

PRODUIT 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.

TABLE DES MATIÈRES

I. FAITS

Le 6 mai 2015, les associations requérantes ont demandé au Gouvernement d'abroger l'article R. 10-13 du code des postes et des communications électroniques (CPCE) et le décret n° 2011-219 du 25 février 2011 comme étant contraires à la Charte des droits fondamentaux de l'Union européenne (la Charte) et à la directive 2002/58/CE de l'Union européenne [1]. Le 6 juillet 2015, le Gouvernement a tacitement refusé d'abroger ces dispositions (section 1) alors même qu'un double changement de circonstances l'exigeait (section 2 page 4).

1. Refus d'abrogation des dispositions litigieuses

Les associations requérantes ont demandé au Gouvernement d'abroger l'article R. 10-13 du code des postes et des communications électroniques (CPCE) et le décret n° 2011-219 du 25 février 2011 en ce qu'ils sont inconventionnels par eux-mêmes ou en ce qu'ils procédent à l'application de dispositions législatives elles aussi inconventionnelles.

1.1. Article R. 10-13 du code des postes et des communications électroniques

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*

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.

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 selon lequel :

« I.-En application du III de l'article L. 34-1 les opérateurs de communications électroniques conservent pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales :

a) Les informations permettant d'identifier l'utilisateur ; b) Les données relatives aux équipements terminaux de communication utilisés ; c) Les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ; d) Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ; e) Les données permettant d'identifier le ou les destinataires de la communication.

« II.-Pour les activités de téléphonie l'opérateur conserve les données mentionnées au II et, en outre, celles permettant d'identifier l'origine et la localisation de la communication.

« III.-La durée de conservation des données mentionnées au présent article est d'un an à compter du jour de l'enregistrement.

« IV.-Les surcoûts identifiables et spécifiques supportés par les opérateurs requis par les autorités judiciaires pour la fourniture des données relevant des catégories mentionnées au présent article sont compensés selon les modalités prévues à l'article R. 213-1 du code de procédure pénale. »

1.2. 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

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. Ce décret liste les données que les opérateurs sont tenus de conserver et détermine leur durée de conservation ainsi que les modalités des demandes administratives de communication de ces données.

Le 6 juillet 2015, le Gouvernement a tacitement refusé d'abroger les dispositions réglementaires litigieuses alors même qu'un double changement de circonstances l'exigeait.

2. Changements 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. Le Parlement français adoptait ainsi 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 l'article L. 32-3-1 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. Cette directive a fait l'objet d'une transposition en droit français par le décret n° 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques créant notamment l'article R. 10-13 CPCE en application de l'article L. 34-1 CPCE.

À l'époque, nombreuses furent les critiques dénonçant l'incompatibilité de ces dispositions avec le respect des droits fondamentaux. 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).

Aujourd'hui, près de dix ans après l'adoption de la directive 2006/24/CE, l'examen de la légalité des dispositions mettant en place un régime de conservation généralisé et indifférencié des « données techniques » fait face à un double changement de circonstances :

– sur le plan technique d'une part, avec la forte augmentation de l'utilisation des technologies de l'information et de la communication ainsi que des nombreuses données techniques ainsi produites, lesquelles révèlent efficacement et avec une grande précision des pans entiers de la vie privée de chaque individu ;
Cette évolution technique a déjà été reconnue notamment par M. le rapporteur public Edouard Crepey qui, lors de l'audience publique tenue devant votre juridiction le 1er juin 2015 dans le cadre de l'affaire n° 388134 ayant donné lieu à la décision FDN et al. du 5 juin 2015, déclarait :

> « la summa divisio entre accès de données et accès de contenus n'a probablement plus la même portée qu'il y a quelques années, et sans doute l'ingérence dans la vie privée que constitue l'accès aux données de connexion doit être réévaluée ».

– sur le plan juridique d'autre part, avec l'arrêt *Digital Rights* de la grande chambre de la Cour de Justice (CJUE).

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 déclare dans l'arrêt *Digital Rights* que ladite directive est invalide car contraire à la Charte des droits fondamentaux de l'Union européenne.

Par cet arrêt historique, la Cour a rejeté le principe d'une conservation généralisée des données relatives 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 » (§ 58).

Cette décision produit depuis une véritable « onde de choc », entraînant de multiples décisions des juridictions de différents États membres qui tour à tour invalident les dispositions nationales en la matière.

– Ainsi, en juin 2014, la Cour constitutionnelle autrichienne a déclaré invalide la majeure partie de la loi nationale. Les opérateurs ont immédiatement cessé de conserver les données concernées.
– Le 3 juillet 2014, la Cour constitutionnelle slovène a annulé la décision de conservation des données. Les trois griefs principaux soulevés par la Cour sont la conservation massive et sans discrimination des données d'une partie significative de la population sans justification, l'absence de motivation de la durée de conservation (8 mois pour les données de connexion à Internet), l'utilisation pour d'autres motifs que les « crimes sérieux ».
– En Roumanie, la première loi de transposition nationale avait été invalidée par la Cour constitutionnelle dès 2009. Le Gouvernement avait adopté une nouvelle loi en 2012. Le 8 juillet 2014, la Cour constitutionnelle a déclaré que la loi de 2012 était également inconstitutionnelle.
– En Bulgarie, la Cour constitutionnelle a déclaré la loi nationale inconstitutionnelle le 12 mars 2015.
– Aux Pays-Bas, la loi néerlandaise imposait une conservation des données pour une durée de 6 à 12 mois, avec des durées différentes selon les types de données. Suite au recours d'une coalition d'ONG, le 11 mars 2015, le tribunal de première instance de La Haye a donné raison à la société civile et a invalidé la loi de 2009 en matière de conservation des données.
– Enfin, en Belgique, la Cour constitutionnelle a jugé le 12 juin 2015 que la loi de transposition nationale, adoptée en juillet 2013, « par identité de motifs avec ceux qui ont amené la Cour de justice de l'Union européenne à juger la directive "*conservation des données*" invalide », et en particulier en raison du caractère généralisé et indifférencié de la conservation, le législateur avait violé la Charte des droits fondamentaux et, partant, la Constitution belge.

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, 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 du 25 février 2011 en ce que, principalement, ceux-ci 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 des droits fondamentaux de l'Union européenne et à la directive 2002/58/CE.

II. DISCUSSION

La Charte des droits fondamentaux de l'Union européenne (la Charte), en son article 52, et la Convention de sauvegarde des droits de l'Homme et des libertés fondamentales (la Convention EDH), en ses articles 8 et 10, exigent que toutes ingérences au droit au respect de la vie privée et à la liberté d'expression soient prévues par la loi, poursuivent un objectif d'intérêt général et soient strictement nécessaires à la poursuite de cet objectif.

Les dispositions litigieuses susvisées mettent en place une ingérence dans les droits et libertés fondamentaux de la quasi-totalité de la population (section 1) qui, au regard de ses finalités (section 2 page 10), n'est ni adéquate (section 3 page 11) ni nécessaire (sections 4 page 15 et 5 page 19).

Selon les requérantes, le caractère inconventionnel de ces dispositions, et *a fortiori* du refus d'en abroger les parties réglementaires, est rendu manifeste par l'arrêt *Digital Rights* du 8 avril 2014 de la Cour de justice déclarant la directive 2006/24/CE contraire à la Charte. Il n'en demeure pas moins que, à l'instar de deux juridictions suédoise et britannique, le Conseil d'État est tenu de transmettre à la Cour de justice de l'Union européenne une ou plusieurs questions préjudicielles afin d'en obtenir des précisions sur l'interprétation et les conséquences devant être données à l'arrêt *Digital Rights* (section 6 page 21).

1. Une ingérence dans les droits fondamentaux d'une vaste ampleur et d'une particulière gravité

La gravité de l'ingérence constituée par les dispositions attaquées est au moins aussi importante que celle caractérisée par la Cour de justice concernant la directive 2006/24/CE.

1.1. La gravité de l'ingérence constituée par la directive 2006/24/CE

L'article 3 de la directive 2006/24/CE, déclarée contraire à la Charte par la Cour de justice 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).

Afin de déterminer le champ des acteurs concernés par ces obligations, il convient notamment de se référer à l'article 2 de la directive « cadre » 2002/21/CE du 7 mars 2002 [1], au considérant 10 de cette directive [2], à la jurisprudence venant préciser la notion de service de communications électroniques [3] ainsi qu'aux décisions rendues par l'Autorité de régulation des communications électroniques et des postes (ARCEP) [4].

Dès lors, il apparaît que la directive imposait une obligation de conservation généralisée à toute personne exploitant un réseau de communications électroniques (tel que certains fournisseurs d'accès à Internet) ou assurant pour le public la transmission de signaux sur ces réseaux (tel qu'un service de messagerie électronique ou de discussion vocale), à l'exclusion des personnes hébergeant ou éditant des contenus accessibles au public (tels que les hébergeurs ou éditeurs de sites internet).

L'obligation de conservation concernait toutes les données générées ou traitées par ces acteurs et qui permettaient de connaître l'auteur, le destinataire, la date, l'heure, la durée, le type et le matériel de chaque communication, telles que les définissait l'article 5 de la directive 2006/24/CE.

Du constat du champ personnel et matériel de cette obligation, la Cour de justice a ainsi caractérisé l'ingérence instituée par un tel régime de conservation dans son arrêt *Digital Rights* :

« 37. Force est de constater que l'ingérence que comporte la directive 2006/24 dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte s'avère, ainsi que l'a également relevé M. l'avocat général notamment aux points 77 et 80 de ses conclu-

1. Un « services de communications électroniques » est défini par la directive 2002/21/CE, article 2, c), comme un « service fourni normalement contre rémunération qui consiste entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques [...] mais qui exclut les services consistant à fournir des contenus à l'aide de réseaux et de services de communications électroniques ou à exercer une responsabilité éditoriale sur ces contenus ».

2. 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, disposant que « les services de téléphonie vocale et de transmission de courrier électronique sont couverts par la présente directive ».

3. 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 finaux de la transmission du signal qui garantit à ces derniers la fourniture du service auquel ils se sont abonnés. »

4. L'ARCEP a qualifié certains services dits « de voix sur IP » ou encore « VoIP », tels que certains services fournis par l'entreprise Skype, de services de communications électroniques (Voir notamment : ARCEP, Skype refuse de se déclarer en tant qu'opérateur, Arcep.fr, 12 mars 2013).

sions, d'une ***vaste ampleur*** *et qu'****elle doit être considérée comme particulièrement grave****. En outre, 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****. [...] »*

« 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****. »*

Il faut souligner que, ce faisant, la Cour de justice n'exclut pas pour autant que les dispositions visées constituent également une ingérence dans l'exercice de la liberté d'expression, telle que reconnue à l'article 11 de la Charte, qui est nécessairement remise en cause par le sentiment d'être surveillé de façon constante.

En atteste une jurisprudence bien établie de la Cour européenne des droits de l'homme (Cour EDH) relative à l'article 10 de la Convention EDH et considèrant que toute loi instaurant des mesures de surveillance des communications :

« crée par sa simple existence, pour tous ceux auxquels on pourrait l'appliquer, une menace de surveillance entravant forcément la liberté de communication entre usagers des services des postes et télécommunications »
(CEDH, Klass et autres c. Allemagne, *Plén., 6 septembre 1978, n° 5029/71, §41 ; voir aussi CEDH* Leander c. Suède, *26 mars 1987, n° 9248/81, §48 ;* Rotaru c. Roumanie, *4 mai 2000, n° 28341/95, §46).*

1.2. La gravité de l'ingérence constituée par les dispositions françaises

Les dispositions législatives françaises établissent un régime de conservation généralisée similaire ou plus large et instituent dès lors une ingérence identique ou plus importante dans les droits fondamentaux de la quasi-totalité de la population.

En effet, tout d'abord, 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 exactement les mêmes personnes que visait l'obligation de conservation de la directive 2006/24/CE : celles exploitant un réseau de communications et celles assurant pour le public la trans-

mission, l'émission ou la réception de signaux sur ces réseaux, à l'exclusion de celles hébergeant ou éditant des contenus accessibles au public.

Les données concernées par cette obligation sont toutes celles qui, traitées par les opérateurs et concernant n'importe quelle personne, « 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 », telles que définies par l'article L. 34-1, VI, du CPCE et recouvrent ainsi exactement 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 Cour de justice concernant cette directive.

Ensuite, 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 — qui sont aussi des opérateurs et étaient donc visés par la directive 2006/24/CE — et des hébergeurs de contenus accessibles au public — qui ne sont pas des opérateurs et étaient donc 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 quelle personne et permettent d'identifier celle-ci.

Dès lors, le régime de conservation établi par l'article 6, II, de la LCEN dépasse celui qu'avait établi la directive 2006/24/CE en ce qu'il s'impose à des acteurs qui étaient exclus de ce dernier — les hébergeurs —, recouvrant ainsi des catégories de données qu'il ne pouvait concerner — telles que celles permettant d'identifier toute personne contribuant à la création d'un contenu diffusé sur Internet.

L'ingérence autorisée par l'article 6, II, de la LCEN dans les droits et libertés des citoyens est donc, concernant les fournisseurs d'accès à internet, semblable à celle caractérisée par la Cour de justice concernant cette directive et, concernant les hébergeurs, distincte de cette ingérence.

En conclusion, le régime français de conservation généralisée de données, résultant de la combinaison des articles L. 34-1, III, du CPCE et 6, II, de la LCEN, autorise une ingérence dont la nature et l'ampleur recouvrent et dépassent celles de l'ingérence qu'autorisait la directive de 2006.

2. Des finalités absentes ou particulièrement larges

Comme l'exige l'article 52, paragraphe 1 de la Charte des droits fondamentaux, la Cour de justice, dans l'arrêt *Digital Rights*, identifie la finalité poursuivie par la directive afin, d'abord, de s'assurer que cette finalité réponde à un besoin d'intérêt général et afin,

ensuite, de pouvoir examiner à son regard la proportionnalité de l'ingérence instituée. Ainsi, la Cour constate que la finalité de la directive 2006/24/CE visait :

> *« [...] garantir la disponibilité de ces données à des fins de recherche, de détection et de poursuite d'**infractions graves** telles qu'elles sont définies par chaque État membre dans son droit interne. L'objectif matériel de cette directive est, dès lors, de contribuer à la lutte contre la criminalité grave et ainsi, en fin de compte, à la sécurité publique. »*

Or, en l'espèce, les dispositions litigieuses ne poursuivent pas un objectif identique.

Tout d'abord, l'article L. 34-1, III, premier alinéa, du CPCE énonce les finalités pour lesquelles le pouvoir réglementaire peut exiger des opérateurs qu'ils conservent les données de connexion de leurs abonnés.

Il s'agit soit « de la recherche, de la constatation et de la poursuite des infractions pénales », soit de la sanction des manquements à l'obligation de veiller à ce qu'un accès à des services de communication au public en ligne n'ait pas été utilisé à des fins de contrefaçons.

Ainsi, là où la directive ne visait que la lutte contre la criminalité grave, le droit français vise la répression de toute infraction pénale, voire la répression de manquements à des obligations administratives.

Les dispositions de l'article L. 34-1 poursuivent donc des finalités particulièrement vastes, couvrant et dépassant celles poursuivies par la directive 2006/24/CE. Dès lors, l'ingérence que ces dispositions instituent doivent être soumises à un **contrôle de proportionnalité d'autant plus strict**.

Ensuite, l'article 6, II, de la LCEN prévoit une obligation de conservation de données à la charge des fournisseurs d'accès à Internet et hébergeurs sans indiquer **la poursuite d'aucune finalité**. L'ingérence qu'il institue ne peut donc être strictement nécessaire à la poursuite d'un objectif légitime, ce dernier n'existant pas — ce qui est manifestement contraire à l'article 52, paragraphe 1, de la Charte.

Tout contrôle de proportionnalité étant ainsi impossible à réaliser, l'ingérance ne saurait être proportionnelle au regard des exigences de la Charte.

Dès lors, l'article 6, II, de la LCEN doit être déclaré contraire à la Charte. Partant, le refus du Gouvernement d'abroger le décret n° 2011-219 pris en son application doit être annulé.

3. L'inaptitude de la conservation généralisée des données à réaliser l'objectif poursuivi

Dans son arrêt, la Cour de justice estime que la conservation généralisée et indifférenciée des données techniques répond de manière adéquate à l'objectif poursuivi.

> *« 49. En ce qui concerne la question de savoir si la conservation des données est apte à réaliser l'objectif poursuivi par la directive 2006/24, il convient de constater que, eu égard à l'importance croissante des moyens de communication électronique, les données qui doivent être conservées en application de cette directive permettent aux autorités*

nationales compétentes en matière de poursuites pénales de disposer de possibilités supplémentaires d'élucidation des infractions graves et, à cet égard, elles constituent donc un instrument utile pour les enquêtes pénales. Ainsi, la conservation de telles données peut être considérée comme apte à réaliser l'objectif poursuivi par ladite directive. »

Néanmoins, on peut regretter que la Cour motive si succintement que la conservation généralisée de données soit apte à contribuer à la poursuite des infractions pénales, alors que cette aptitude n'a jamais été effectivement établie (cf. section 3.1). À l'inverse, il est établi notamment par les autorités britaniques que la conservation des données induit de nombreuses erreurs pouvant avoir de très graves conséquences (cf. section 3.2 page suivante).

3.1. L'absence de preuve de l'aptitude des mesures contestées à réalisée l'objectif poursuivi

Ni la Commission européenne ni aucune autorité nationnale n'a fait état d'aucun élément de fait au soutien du constat selon lequel la conservation généralisée des données serait adéquate pour atteindre l'objectif poursuivi.

Or, par principe, étant face à une ingérence grave dans les droits et libertés fondamentaux, la charge de la preuve de son adéquation à l'objectif poursuivi repose nécessairement sur la personne s'en prévalant — en l'espèce, le législateur français. L'adéquation de la conservation généralisée des données à l'objectif qu'elle poursuit ne peut être présumée.

Au niveau européen, le Contrôleur européen de la protection des données a déjà fait apparaître en 2011 les lacunes des justifications avancées pour la mise en place de systèmes de conservation des données :

> « Bien que la Commission ait clairement consenti bon nombre d'efforts dans la collecte d'informations auprès des gouvernements des États membres, les informations quantitatives et qualitatives fournies par les États membres ne sont pas suffisantes pour confirmer la nécessité de la conservation des données telle qu'arrêtée par la directive sur la conservation des données. Des exemples intéressants de son utilisation ont été fournis, mais **il y a tout simplement trop de lacunes dans les informations présentées dans le rapport pour pouvoir tirer des conclusions générales sur la nécessité de l'instrument**. »
>
> (Contrôleur européen de la protection des données, *Avis sur le rapport d'évaluation de la Commission au Conseil et au Parlement européen concernant la directive sur la conservation des données (directive 2006/24/CE),* JOUE, C 279 du 23 septembre 2011, pp. 1 et s., point 44, `https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2011/11-05-30_Evaluation_Report_DRD_FR.pdf`)

Jamais le législateur français n'a justifié dans une étude d'impact ou autre rapport de l'utilité d'une telle ingérence dans les droits et liberté des citoyens. Pourtant, un tel moyen aurait permis au Gouvernement de rendre compte, ne serait-ce que partiellement, de l'adéquation du dispositif engagé.

Or, trois études indépendantes réalisées en 2005, 2008 et en 2012, démontrent l'inaptitude d'un régime de conservation des données à poursuivre l'objectif de lutter contre la criminalité.

D'après une étude conduite à la demande du Gouvernement allemand, l'absence de régime de rétention générale des données n'a qu'une incidence très faible sur les demandes de données émanant de la police. Par rapport à l'ensemble des enquêtes pénales, moins de 0,01% des procédures d'enquêtes criminelles furent affectées potentiellement par l'impossibilité d'accéder à des données de connexion. [5]

Une étude néerlandaise a également démontré l'inaptitude d'un régime de conservation générale des données à déterminer le succès d'une enquête. [6]

Enfin, une étude de l'Institut Max Planck de 2012, réalisée à la demande du ministère de la justice allemand, rappelle là encore que la démonstration de l'aptitude d'un régime de conservation généralisée des données n'a pas été faite. Cette étude, focalisée sur l'Allemagne ainsi que sur la Suisse, démontre au contraire que la loi de rétention des données n'a **pas d'impact sur le taux d'élucidation des crimes sérieux**. [7]

En conclusion, en l'absence de preuve de la part du législateur, du Gouvernement ou de quelconque autorité publique de l'adéquation du dispositif, celle-ci ne peut être présumée et doit donc être considérée comme absente. En sus de ne rien apporter à la quasi-totalité des enquêtes, la conservation généralisée des données entraîne de nombreuses erreurs causant parfois de lourds préjudices.

3.2. Les erreurs engendrées par la conservation généralisée des données

Le régime de conservation généralisée engendre de nombreuses erreurs entrainant la transmission à l'administration de données personnelles concernant des innocents ainsi que l'imputation à ces derniers d'actes les plus graves.

Pour en attester, il convient de se référer au rapport produit en juillet 2015 par le commissaire britannique en charge de l'interception des communications. Les raisons obligeant à se référer à un rapport étranger sur cette question sont, d'une part, qu'au Royaume-Uni les autorités traitant ces données sont dans l'obligation de communiquer les erreurs commises à un contrôleur et, d'autre part, que ce même contrôleur est tenu, contrairement aux autorités françaises, de faire des rapports bi-annuels au Parlement britannique sur la mise en œuvre des interceptions et la conservation des données [8].

5. Institut Max Planck, The Right of Discovery Concerning Telecommunication Traffic Data According to §§ 100g, 100h of the German Code of Criminal Procedure, March 2008, `http://dip21.bundestag.de/dip21/btd/16/084/1608434.pdf`, p. 150.

Voir aussi, Starostik, 17 mars 2008, `http://www.vorratsdatenspeicherung.de/images/schriftsatz_2008-03-17.pdf`, p. 2.

6. Erasmus University Rotterdam, Who retains something has something, 2005, `http://www.erfgoedinspectie.nl/uploads/publications/Wie%20wat%20bewaart.pdf`, p. 28

7. Albrecht, Hans-Jörg & Kilchling, Michael (Hrsg.) : *Schutzlücken durch Wegfall der Vorratsdatenspeicherung ? Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsverkehrsdaten.* Kriminologische Forschungsberichte aus dem Max-Planck-Institut, Bd. K 160. Duncker & Humblot, Berlin 2012 (im Erscheinen). `https://www.mpicc.de/de/forschung/forschungsarbeit/kriminologie/vorratsdatenspeicherung.html`

8. Voir le dernier rapport :`http://www.iocco-uk.info/docs/2015%20Half-yearly%20report%20%`

Ainsi, le contrôleur britannique fait savoir dans son dernier rapport que, en 2014, ce sont 998 erreurs qui lui ont été rapportées par les autorités britanniques. Il offre même une vue synthétique d'une grande transparence sur les différentes catégories d'erreurs commises [9]. Ces erreurs ne sont pas dues à des erreurs d'interprétation de la donnée par l'administration, mais à des erreurs dans la demande ou la transmission de ces données. C'est à dire que, plus de deux fois par jour, en moyenne, des données concernant une personne innocente sont transmises aux autorités publiques, révélant leur vie privée, alors qu'aucune suspicion ne justifiait cette transmission.

Ces transmission, relevant davantage de l'erreur technique, sont la conséquence directe de ce que l'administration a accès à un nombre trop important de données. En effet, seule la conservation, en amont, de données ne concernant que des personnes ciblées permettrait de réaliser des demandes et des transmissions suffisamment précises pour éviter les erreurs et permettre de surveiller efficacement les personnes devant effectivement l'être.

Sur ce millier d'erreurs commises au Royaume-Uni, dix-sept cas particulièrement graves ont été reportés pour la seule année 2014, c'est-à-dire plus d'un cas particulièrement grave par mois. Il ne s'agit pas seulement de simples ingérences dans la vie privée, mais également d'actes particulièrement graves, notamment la fouille de domiciles ou des accusations de pédopornographie. Selon le contrôleur britannique, ces erreurs auraient pu avoir un effet dévastateur pour les personnes injustement mises en cause.

En France, aucune information n'existe pour établir l'aptitude de la conservation des données à participer à la réalisation des objectifs fixés ou permettre d'attester de ses dangers. Si le rapport d'activité pour l'année 2013 de la CNCIS fait apparaître le nombre très élevé de demandes traitées par le groupe interministériel de contrôle – 321.243 [10] – il ne fait pas apparaître le nombre d'erreurs dans le traitement des données liées à ces demandes.

Cette lacune est hautement condamnable en ce qu'elle interdit toute transparence sur les cas où la conservation systématique des données a conduit à l'accusation d'innocents.

En l'absence de toute information à ce sujet, il n'y a aucune raison de penser que le système français est immunisé contre de telles erreurs. Au contraire, en l'absence de mécanismes de vigilances ou de publication de propositions d'améliorations par les contrôleurs de ce dispositif [11], il y a toutes les raisons de penser que de telles erreurs sont également commises en France.

En conclusion, là où il n'est apporté aucune preuve de l'adéquation de la conservation généralisée des données à l'objectif poursuivi, il est au contraire avéré qu'elle entraîne l'accusation de personnes innocentes, risque encore aggravé par le caractère systématique de la conservation des données.

`28web%20version%29.pdf`

9. Voir p. 16 du rapport.
10. Voir p. 96 du rapport.
11. Voir *contra* le rapport du commissaire britannique.

4. L'absence de règles claires et précises assurant la stricte nécessité de l'ingérence

La directive 2006/24/CE a été invalidée par la Cour de justice en ce qu'elle ne prévoyait « pas de règles claires et précises régissant la portée de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte » (point 65 de l'arrêt *Digital Rights*) et manquait ainsi « de garantir qu'elle [était] effectivement limitée au strict nécessaire ». Cette exigence de nécessité à laquelle doit se conformer toute ingérence dans les droits fondamentaux est fondée aussi bien sur l'article 52, paragraphe 1 de la Charte des droits fondamentaux que sur une jurisprudence constante de la Cour EDH et de la Cour de justice.

Venant préciser les critères de stricte nécessité qu'elle avait alors dégagés dans l'arrêt *Digital Rights*, la Cour a clairement et limitativement établi, dans son arrêt *Schrems* du 6 octobre 2015 [12] (point 93), que « 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 » sans :

- « qu'aucune différenciation, limitation ou exception soit opérée en fonction de l'objectif poursuivi » (section 4.1) ni ;
- « que soit prévu 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 » (section 4.2 page 17) .

Or, la règlementation française en matière de conservation généralisée des données présente précisément ces deux défauts.

4.1. Le champ des données conservées

Quant à la nécessité de limiter le champ des données conservées, l'arrêt *Schrems* s'inscrit dans une ligne jurisprudentielle déjà définie par la Cour EDH et la Cour de justice. Ainsi, par stricte application de l'article 8 de la Convention EDH, la Cour EDH encadre le champ des données à caractère personnel pouvant être collectées et conservées à des fins d'intérêt général en considérant que :

> *« 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*** *»*
>
> *(Cour EDH, g^de ch. du 4 décembre 2008,* Marper c. Royaume-Uni, *n^os 30562/04 et 30566/04, § 103)*

12. CJUE, 6 octobre 2015, *Maximillian Schrems contre Data Protection Commissioner*, C-362/14

Dans son arrêt *Digital Rights*, la Cour de justice a déduit la réciproque logique de ce principe en établissant que **rendre obligatoire la conservation de données à caractère personnel concernant la quasi-totalité de la population ne peut être strictement nécessaire à la poursuite d'aucun objectif**.

En effet, lors de son examen, la Cour de justice 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. »*

Il ressort ainsi que le caractère strictement nécessaire d'une obligation de conserver des données à caractère personnel dépend de la correspondance entre les données devant être conservées et les données dont l'accès est nécessaire à la poursuite de l'objectif visé. De sorte, dès lors qu'il existe une différence absolue entre les données devant obligatoirement être conservées – lesquelles concernent la quasi-totalité de la population – et les données nécessaires à la poursuite des objectifs visés, l'obligation de conservation généralisée ne peut jamais être strictement nécessaire à la poursuite d'aucun objectif.

Ce même principe est repris par la Cour dans son arrêt *Schrems*.

Selon les requérantes, il convient de constater en référence à ce seul principe l'invalidité des articles des articles L. 34-1, III, du CPCE et 6, II, de la LCEN. En effet, ces articles établissent, à l'instar de la directive 2006/24/CE, une obligation de conservation de données personnelles concernant la quasi-totalité de la population. L'obligation de conservation de données à caractère personnel établie aux articles L. 34-1, III, du CPCE et 6, II, de la LCEN ne peut ainsi être strictement nécessaire à la poursuite d'aucun objectif, et encore moins à la poursuite de l'objectif que lui a donné le législateur — tel

objectif étant, dans un cas, plus lâche que celui défini par la directive invalidée et, dans l'autre, tout simplement indéfini (cf. section 2 page 10).

Néanmoins, le 4 mai 2015, avant que l'arrêt *Schrems* ne soit rendu, la Cour administrative d'appel de Stockholm avait transmis à la Cour de justice la question préjudicielle suivante :

> « Une obligation générale de conservation de données, relative à toute personne et à tous les moyens de communication électronique et portant sur l'ensemble des données relatives au trafic, sans qu'aucune différenciation, limitation ni exception ne soient opérées en fonction de l'objectif de lutte contre la criminalité [telle que décrite dans la décision de renvoi], est-elle compatible avec l'article 15, paragraphe 1, de la directive 2002/58 (1) compte tenu des articles 7, 8 et 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne ? »
> (affaire C-203/15, question publiée au JOUE C 221 du 6 juillet 2015, p. 5)

À cette question s'est depuis ajoutée, une autre question préjudicielle transmise par la cour d'appel du Royaume-Uni le 20 novembre 2015 [13]. Par cette question, la cour britannique demande à la Cour de justice de préciser si les critères énoncés dans la décision *Digital Rights* s'imposent à une législation nationale telle que la législation britannique.

Dès lors, afin de garantir l'application homogène de la Charte dans l'ensemble de l'Union européenne, d'assurer son effet utile et de résoudre la présente affaire dans le respect du principe de coopération loyale — lequel s'impose à l'ensemble des autorités des États membres — votre juridiction devrait, en vertu de l'article 267 du traité sur le fonctionnement de l'Union européenne, transmettre à la Cour de justice la question suivante : **une obligation générale de conserver des données techniques concernant toute personne, sans aucune différenciation, limitation ou exception, est-elle compatible avec l'article 15(1) de la directive 2002/58/CE eu égard aux article 7, 8 et 52(1) de la Charte ?**

De surcroît, et si les articles L. 34-1, III, du CPCE et 6, II, de la LCEN n'étaient pas déclarés comme violant la Charte de ce seul fait, *quod non*, la réglementation française ne manque pas moins aux autres critères exigés par la Cour.

4.2. Les conditions d'accès des autorités publiques aux données conservées

La Cour de justice conditionne la validité des régimes de conservation généralisée à la présence de critères objectifs limitant les finalités que l'autorité publique doit poursuivre pour accéder aux données ainsi conservées. Dans son arrêt *Digital Rights*, elle constatait ainsi que :

> *« 60. [...] la directive 2006/24 ne prévoit aucun critère objectif permettant de délimiter l'accès des autorités nationales compétentes aux données et leur utilisation ultérieure à*

13. Court of Appeal (Civil Division), affaire n° C1/2015/2612, `https://www.judiciary.gov.uk/judgments/secretary-of-state-for-the-home-department-v-david-davis-mp-and-others/`

des fins de prévention, de détection ou de poursuites pénales concernant des infractions pouvant, au regard de l'ampleur et de la gravité de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, être considérées comme suffisamment graves pour justifier une telle ingérence. »

En effet, la directive 2006/24/CE se contentait de limiter l'accès aux données conservées « à des fins de recherche, de détection et de poursuite d'infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne » (article premier de la directive). Ce faisant, elle ne prévoyait aucun critère suffisamment précis pour limiter ces finalités à celles concernant des infractions « suffisamment graves pour justifier une telle ingérence ».

La Cour de justice a repris et précisé ce critère dans son arrêt *Schrems* pour en faire un critère de validité de tout règime de conservation de données. Ainsi, tel régime violerait la Charte pour la seule raison qu'il soit établi sans « que soit prévu **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** ».

En l'espèce, en droit français, c'est au livre VIII du code de la sécurité intérieure (tel qu'il résulte de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement), à son article L. 811-3, que sont prévus les objectifs limitant l'accès par l'administration aux données conservées au titre des dispositions présentement attaquées. Parmi ces objectifs, on trouve notamment la défense et la promotion des « intérêts majeurs de la politique étrangère, [de] l'exécution des engagements européens et internationaux » et des « intérêts économiques, industriels et scientifiques majeurs de la France ».

Or, en premier lieu, de tels objectifs ne correspondent manifestement pas à la seule prévention d'infractions, la loi française échouant donc à prévoir un « critère objectif permettant de délimiter » l'action de l'administration à des infractions « suffisamment graves pour justifier une telle ingérence ». En second lieu, de tels objectifs sont si largement définis, et d'une telle diversité, qu'ils ne peuvent en aucun cas être considérés comme délimités par « un critère objectif [...] à des fins précises, strictement restreintes et susceptibles de justifier l'ingérence ».

Toutefois, si votre juridiction avait un doute sur la contrariété de ces objectifs aux critères qu'en exige la Cour de justice, elle serait dans l'obligation, pour les mêmes raisons que celles énoncées *supra* de transmettre à la Cour de justice une question préjudicielle pouvant être formulée de la manière suivante : **une obligation générale de conserver des données techniques concernant toute personne, sans aucune différenciation, limitation ou exception, et auxquelles les autorités publiques peuvent accéder pour défendre et promouvoir les intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux et les intérêts économiques, industriels et scientifiques majeurs de l'État membre en cause est-elle compatible avec l'article 15(1) de la directive 2002/58/CE, eu égard aux article 7, 8 et 52(1) de la Charte ?**

Votre juridiction s'inscrirait là encore dans la lignée de la Cour administrative d'appel de Stockholm puisque celle-ci a posé en complément de la première question susmentionnée la question suivante :

« S'il est répondu par la négative à la première question, une telle obligation de

conservation peut-elle néanmoins être admise :

« a) si l'accès par les autorités nationales aux données conservées est encadré de la manière précisée [dans la décision de renvoi], et

« b) si les exigences de protection et de sécurité des données sont régies de la manière précisée [dans la décision de renvoi], et que

« c) toutes les données en question doivent être conservées pendant six mois à compter du jour de l'achèvement de la communication avant d'être effacées, comme il l'est exposé [dans la décision de renvoi] ? »

5. L'existence de mesures alternatives plus proportionnées

D'autres mesures pouvant être instaurées permettraient d'atteindre les finalités poursuivies tout en constituant une ingérence moins grave dans les droits et libertés fondamentaux.

Dans son avis de 2011, le Contrôleur européen de la protection des données pouvait déjà s'exprimer comme suit :

> *« Le CEPD reconnaît qu'un système de conservation des données a posteriori implique moins d'informations qu'un système général de conservation des données. Cependant, c'est précisément grâce à sa nature plus ciblée que la conservation des données a posteriori constitue un instrument moins intrusif dans la vie privée en termes de portée et de nombre de personnes concernées. L'évaluation doit non seulement s'intéresser aux données disponibles, mais également aux différents résultats obtenus avec les deux systèmes. Le CEPD estime qu'une étude plus approfondie de cette mesure s'avère justifiée et indispensable. Cela pourrait se faire dans le cadre de l'étude d'impact dans les mois à venir. »(point 56)*
>
> *(Avis du Contrôleur européen de la protection des données sur le rapport d'évaluation de la Commission au Conseil et au Parlement européen concernant la directive sur la conservation des données (directive 2006/24/CE), JOUE, C 279 du 23 septembre 2011, pp. 1 et s., https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2011/11-05-30_Evaluation_Report_DRD_FR.pdf)*

En effet, les régimes de conservation généralisée de données s'opposent en pratique à ceux de conservation sur injonction, circonscrit aux données relatives à un nombre limité de personnes signalées par l'autorité publique aux intermédiaires techniques pertinents.

Il est à regretter que l'étude annuelle produite en 2014 par le Conseil d'État sur « le numérique et les droits fondamentaux » n'ait pas cherché à étudier cette alternative en détails, la déclarant trop rapidement « moins efficace » que la conservation généralisée [14], alors qu'un examen plus précis révèle que, non seulement, il est périlleux d'affirmer cela

14. Étude annuelle 2014 du Conseil d'État, *Le numérique et les droits fondamentaux*, p. 209 : « Toutefois, ce mécanisme de conservation sur injonction serait nettement moins efficace que la conservation systématique du point de vue de la sécurité nationale et de la recherche des auteurs d'infraction. En effet, il ne permettrait aucun accès rétrospectif aux échanges ayant eu lieu avant que l'autorité n'identifie une menace ou une infraction »

quand l'efficacité des mesures en cause n'a jamais été sérieusement évaluée par le législateur (voir section 3.1 page 12) et que, de surcroît, portant des atteintes aux droits et libertés de la population nettement plus faibles, l'existence d'une telle alternative rend par elle-même les dispositions attaquées excessives et non proportionnées aux atteintes qu'elles autorisent.

S'agissant en premier lieu de la gravité de l'ingérence autorisée dans les droits et libertés, la conservation sur injonction n'affecte par nature qu'un nombre objectivement limité de personnes, défini par les besoins pratiques et concrets de la prévention, de la détection et de la poursuite d'infractions graves, et non pas la quasi-totalité de la population, tel que le fait la conservation généralisée (voir section 1 page 7).

En deuxième lieu, s'agissant des finalités poursuivies, la conservation sur injonction, par définition, est limitée à chacune de ses réalisations au motif de l'injonction la faisant naître et, sans avoir même à évaluer dans quelle mesure de tels motifs pourraient être limités au strict nécessaire. En cela, elle poursuit nécessairement des finalités plus précises – car toujours circonstanciées – que la finalité abstraite et, donc, en pratique illimitée de lutte générale contre les infractions (voir section 2 page 10).

En troisième lieu, s'agissant de la plus grande aptitude à atteindre l'objectif poursuivi que la conservation généralisée, l'examen de régimes alternatifs de conservation des données adoptés en Europe est d'une aide précieuse.

Tout d'abord, comme cela a été évoqué précédemment, la conservation généralisée des données est à la source de nombreuses erreurs pouvant causer de graves dommages aux individus. À l'inverse, et par définition, un système de conservation des données sur injonction ne conduit pas au mésusage d'autant de données.

Ensuite, plusieurs États européens, dont l'Autriche, la Belgique, l'Allemagne, la Grèce ou la Roumanie, ont renoncé à recourir à la conservation généralisée des données techniques, préférant des mesures ciblées de conservation des données, parmi lesquelles l'injonction faite par les autorités à un opérateurs de conserver les données ne concernant que certains individus suspects, sans que cela n'ait en aucune façon nui à leur capacité de lutte contre les infractions graves. Ainsi, l'étude précitée de 2008 commanditée par le Gouvernement allemand, conclut à ce que seulement 4% des demandes d'accès de données faites par les autorités n'avaient pu être satisfaites en raison de l'absence d'une obligation de conservation généralisée des données techniques [15], ce qui tend à démontrer qu'en réalité, dans la pratique, un régime de conservation généralisé des données techniques n'est pas nécessaire. Il en va de même de l'étude allemande, elle aussi précitée, réalisée en 2012 par le Max Planck Institute.

Prenant le contre-pied de ces études, en octobre 2015, le chambre basse du Parlement allemand a adopté en première lecture un projet de loi qui, s'il venait à être définitivement adopté, instituerait une conservation généralisée, mais très encadrée des données. S'il tend bien à instaurer un mécanisme de conservation généralisée des données, le dispositif débattu en Allemagne ne conduirait en rien à la remise en cause du constat d'invalidité qui doit être tiré de l'examen du système français. En effet, dans le système allemand encore en débat, la durée de conservation des données ne serait que de quelques semaines

15. Max Planck Institute for Foreign and International Criminal Law, *The Right of Discovery Concerning Telecommunication Traffic Data According to §§ 100g, 100h of the German Code of Criminal Procedure*, March 2008, `http://dip21.bundestag.de/dip21/btd/16/084/1608434.pdf`, p. 150.

et les conditions d'accès aux données ainsi que les modalités de leur conservation seraient très contraintes. Ce projet de loi confirme à tout le moins que le système français n'est en aucune manière proportionné. Il ne remet d'ailleurs pas en cause les constats des études précitées. Pour ce faire, il faudrait par exemple qu'il soit démontré que depuis cinq ans les autorités allemandes ne parviennent pas à résoudre des affaires qui, pour l'être, mériteraient de procéder à la surveillance de l'ensemble de la population. Ce qui n'a jamais été fait jusqu'à présent. Qui plus est, il n'est pas certain que ce projet, présenté avant l'adoption de l'arrêt *Schrems*, lui soit conforme.

En quatrième et dernier lieu, quand à la nécessité, et notamment au regard des critères précis posés par la Cour de justice pour déclarer la directive 2006/24/CE contraire à la Charte de l'Union européenne, la conservation sur injonction s'oppose par nature à ce qu'il n'existe « aucune relation entre les données dont la conservation est prévue et une menace pour la sécurité publique » [16]. De plus, en ce qu'elle limite à la source le volume des données accessibles, elle offre à elle seule une importante garantie de ce que l'autorité publique n'accédera à ces données que pour poursuivre des finalités concernant des infractions « suffisamment graves pour justifier une telle ingérence » [17] ou étant « des fins précises, strictement restreintes » [18].

En conclusion — au regard d'une alternative tout autant si ce n'est plus apte à atteindre l'objectif poursuivi et entraînant des atteintes bien plus faibles dans les droits et libertés fondamentaux des citoyens — les dispositions attaquées, qui établissent un régime de conservation généralisée des données à caractère personnel, sont disproportionnées.

6. L'opportunité d'un renvoi préjudiciel à la Cour de justice

Comme cela a été évoqué (notamment section 4.1 page 17), deux renvois préjudiciels, actuellement pendants devant le Cour de justice, portent déjà sur l'interprétation de la Charte et des critères mis en avant par la Cour dans la décision *Digital Rights* quant à la validité des dispositifs de conservation des données. Dans ce contexte, les requérantes insistent sur le fait que l'opportunité d'un renvoi préjudiciel est manifeste, pour au moins deux questions.

6.1. La légalité d'une obligation générale de conservation des données sans différenciation, limitation, ni exception

Afin de garantir l'application homogène de la Charte sur l'ensemble du territoire de l'Union européenne, d'assurer son effet utile et de résoudre la présente affaire dans le respect du principe de coopération loyale – lequel s'impose à l'ensemble des autorités des États membres – votre juridiction devrait à tout le moins, en vertu de l'article 267 du traité sur le fonctionnement de l'Union européenne, transmettre à la Cour de justice la question suivante : **une obligation générale de conserver des données techniques**

16. CJUE, *Digital Rights*, précité, § 59
17. CJUE, *Digital Rights*, précité, § 60
18. CJUE, *Schems*, précité, § 93

concernant toute personne, sans aucune différenciation, limitation ou exception, est-elle compatible avec l'article 15(1) de la directive 2002/58/CE eu égard aux article 7, 8 et 52(1) de la Charte ?

6.2. Le contour des objectifs justifiant l'accès aux données techniques

Comme énoncé *supra*, votre juridiction pourra aussi transmettre à la Cour de justice une question préjudicielle pouvant être formulée de la manière suivante : **une obligation générale de conserver des données techniques concernant toute personne, sans aucune différenciation, limitation ou exception, et auxquelles les autorités publiques peuvent accéder pour défendre et promouvoir les intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux et les intérêts économiques, industriels et scientifiques majeurs de l'État membre en cause est-elle compatible avec l'article 15(1) de la directive 2002/58/CE, eu égard aux article 7, 8 et 52(1) de la Charte ?**

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 26 novembre 2015, à Paris

Pour l'association
French Data Network,
pour l'association
La Quadrature du Net,
et pour la
Fédération des fournisseurs d'accès à Internet associatif,
le mandataire unique,
Benjamin Bayart