Conseil d'État
Section du contentieux
10e chambre
N° 393099

Mémoire en réplique

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 : contact@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. PROCÉDURE

En réponse au mémoire en défense du 20 juin 2016 déposé par le ministre de la justice, garde des sceaux, les associations French Data Network (FDN), La Quadrature du Net ainsi que la Fédération des fournisseurs d'accès à Internet associatifs (FFDN) entendent verser aux débats les observations suivantes.

Persistant dans l'ensemble des moyens et des conclusions qu'elles ont développés dans leurs précédentes écritures, les exposantes entendent plus particulièrement souligner la lecture partielle et erronée faite par la partie défenderesse du droit applicable en l'espèce.

II. DISCUSSION

1. Sur les demandes de questions préjudicielles

Les associations requérantes ont demandé au Conseil d'État de transmettre deux questions préjudicielles à la Cour de justice de l'Union européenne (ci-après la Cour de justice, ou CJUE). Le ministre estime que la première de ces questions est identique à une des questions posées dans l'affaire C-203/15, actuellement pendante devant la Cour de justice. De toute évidence, les parties requérantes n'ignorent aucunement cette procédure à laquelle elles ont elles-mêmes fait référence.

À défaut d'avoir permis aux parties requérantes de se joindre à la procédure actuellement en cours devant la Cour de justice dans les affaires jointes C-203/15 et C-698/15 *Tele2, Watson et al.*, le Conseil d'État ne saurait trancher le présent litige sans attendre leur issue finale. Les conclusions présentées le 19 juillet 2016 par l'avocat général Saugmandsgaard Øe dans ces deux affaires jointes confirment cette nécessité (CJUE, 19 juill. 2016, *Conclusions de l'avocat général Saugmandsgaard Øe*, C-203/15, C-698/15).

2. Sur l'atteinte à la liberté d'expression

Contrairement à ce qu'affirme le ministre de la justice (p. 7 de son mémoire), la Cour de justice n'a pas « écarté l'article 11 de la Charte des droits fondamentaux » avant de conclure à la violation des articles 7 et 8 de la Charte. Au contraire, la Cour de justice considère dans l'arrêt *Digital Rights Ireland* que le régime instauré par la directive 2006/24/CE « soul[evait] des questions relatives à la protection tant de la vie privée que des communications consacrée à l'article 7 de la Charte à la protection des données à caractère personnel prévue à l'article 8 de celle-ci ainsi qu'au respect de la liberté d'expression garantie par l'article 11 de la Charte. » (CJUE, g^{de} ch., 8 avr. 2014, *Digital Rights Ireland*, C-293/12, C-594/12, point 25)

Dans ce même arrêt *Digital Rights Ireland*, la Cour de justice précise ensuite que « il n'est pas exclu que la conservation des données en cause

puisse avoir une incidence sur l'utilisation, par les abonnés ou les utilisateurs inscrits, des moyens de communication visés par cette directive et, en conséquence, sur l'exercice par ces derniers de leur liberté d'expression, garantie par l'article 11 de la Charte. » (point 28)

Et ce n'est qu'après avoir conclu à l'invalidité de la directive au regard des articles 7 et 8 de la Charte qu'elle considère que, « dans ces conditions, il n'y a pas lieu d'examiner la validité de la directive 2006/24 au regard de l'article 11 de la Charte. » (point 70)

Mais à aucun moment l'atteinte à la liberté d'expression n'est considérée comme pouvant être évacuée. Or, c'est là un élément décisif avancé par les associations requérantes : la conservation généralisée induit une très forte restriction de la liberté d'expression des individus en plus de constituer une atteinte à leur vie privée et à la protection de leurs données personnelles.

3. Sur l'objectif d'intérêt général susceptible de justifier la conservation généralisée des données

Dans son mémoire en défense, le ministre de la justice indique (p. 8) que, dans son arrêt *Digital Rights Ireland*, la CJUE considère que l'obligation de conservation généralisée « répond à un objectif d'intérêt général » mais prétend que « les requérantes [l']omettent totalement ».

Pourtant, les associations requérantes ont explicitement indiqué dans leurs précédentes écritures que la Cour de justice avait effectivement reconnu que la conservation généralisée des données poursuivait un objectif d'intérêt général — celui de lutter contre les infractions graves (voir le premier mémoire complémentaire des associations requérantes, pp. 10 et 11). Et c'est précisément au regard de cet objectif que les requérantes ont contesté la conformité des finalités poursuivies par les dispositions françaises attaquées.

Dans ses conclusions rendues le 19 juillet 2016, l'avocat général Saugmandsgaard Øe confirme d'ailleurs que si une conservation généralisée des données était admise — ce que les associations requérantes contestent — celle-ci ne pourrait servir que « l'objectif de lutte contre les infractions graves » (point 174). Or, cela n'est aucunement le cas du système français, lequel s'étend à n'importe quelle poursuite ou finalités que les autorités publiques jugent bonnes de poursuivre (cf. section 2 page 10 du mémoire complémentaire du 26 novembre 2015).

Dans ses écritures, le ministre prétend que l'obligation de conservation généralisée française ne poursuit qu'une seule finalité, celle de « garantir la disponibilité de ces données à des fins de recherche, de détention et de poursuite d'infractions graves » (p. 8).

Pourtant, tel que déjà relevé par les associations requérantes, la lettre des dispositions françaises attaquées ne limite aucunement les finalités

poursuivies à la lutte contre les infractions graves :

— d'un côté, l'article L. 34-1 CPCE concerne la lutte contre tout type « [d']infractions pénales » et,
— de l'autre, l'article 6 de la LCEN concerne n'importe quelle finalité poursuivie par l'autorité judiciaire, sans aucune restriction.

Il en va de même des finalités qui sont effectivement poursuivies par cette conservation généralisée au regard d'autres dispositions françaises. Ainsi, l'article L. 851-1 du code de la sécurité intérieure prévoit que les services de renseignement peuvent collecter toutes les données concernées par cette obligation de conservation afin de poursuivre l'un des objectifs définis à l'article L. 811-3 du même code. Parmi ces objectifs, nombreux sont parfaitement étrangers à la lutte contre les infractions graves, tels que la défense des intérêts majeurs de la politique étrangère de la France, de l'exécution de ses engagements européens et internationaux ou de ses intérêts économiques, industriels et scientifiques majeurs.

Ainsi, lorsque le ministre de la justice prétend que l'ingérence permises par les dispositions attaquées « poursuit un objectif d'intérêt général éminent » (p. 11) en se référant à celui de lutte contre les infractions graves, il ne fait que souligner le caractère erroné d'une telle prétention.

4. Sur les critères établis par la Cour de justice permettant d'établir la stricte nécessité d'un régime de conservation des données

De manière préliminaire, les associations requérantes insistent sur le fait qu'elles ne contestent pas toute forme de conservation des données permettant de lutter contre les infractions graves. La conservation des données peut revétir de multiples formes : elle peut être généralisée ou ciblée ; de plus ou moins longue durée ; respectueuse ou non de certains contrôles et d'une forme d'équilibre institutionnel. Les données collectées peuvent ensuite être plus ou moins sécurisées, etc.

À la différence de nombreux autres régimes européens de conservation des données, le système français cumule toutes les violations possibles au droit européen : il est généralisé, la durée de conservation est inutilement longue, les données ne sont pas suffisamment sécurisées eu égard à leur caractère hautement sensible et intrusif et à l'amplitude de la conservation, enfin, l'accès aux données n'est pas encadré et aucun contrôle judiciaire préalable et indépendant n'est exercé tant sur la conservation par les opérateurs que sur l'accès aux données par la police administrative.

Ce que les associations requérantes demandent au Conseil d'État de juger en premier lieu comme n'étant pas nécessaire, entraînant ainsi la disproportion et l'invalidité du système français, est le principe instauré en droit français et mis en œuvre par les dispositions attaquées d'une

conservation généralisée des données de connexion de l'ensemble de la population, soit l'obligation faite aux fournisseurs d'accès à Internet et hébergeurs de tenir, pour le compte des autorités publiques nationales, un journal de surveillance de l'ensemble de la population.

Une lecture rigoureuse de la jurisprudence de la Cour de justice invalide la position défendue par le Gouvernement selon laquelle le régime français de conservation généralisée des données peut être considéré comme limité au strict nécessaire.

En droit, la Cour de justice a dégagé trois critères permettant chacun de considérer si un régime de conservation et d'accès aux données est limité ou non au strict nécessaire au regard à la fois des articles 7 et 8 de la Charte (voir CJUE, g^{de} ch., 8 avr. 2014, *Digital Rights Ireland*, C-293/12, C-594/12, points 57 à 65 [1] et CJUE, g^{de} ch., 6 oct. 2015, *Schrems*, C-362/14 point 93).

En premier lieu, n'est pas limité au strict nécessaire un régime de conservation généralisée des données sans limitation, différenciation ni exception (CJUE, g^{de} ch., 8 avr. 2014, *Digital Rights Ireland*, C-293/12, C-594/12, point 57).

La Cour précise que de telles limitation, différenciation ou exceptions doivent se faire en fonction de l'objectif poursuivi, c'est-à-dire la lutte contre la criminalité grave.

La Cour caractérise une telle absence de limitation, différenciation ou exception comme une « absence générale de limite » (point 60). Partant, l'importance de ce critère ne saurait être minimisée comme le fait le ministre dans son mémoire en réponse lorsqu'il affirme qu' « il n'est pas possible d'opérer *a priori* une différenciation, limitation ou exception dans la conservation des données de connexion en fonction de l'objectif de lutte contre les infractions graves [...] » (p. 9 du mémoire en défense).

La Cour détaille pourtant le type de limites qui peuvent être considérées comme réduisant au strict nécessaire un régime de conservation de données, par exemple lorsque les mesures de conservation portent « 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. » (point 59)

À cet égard, l'argumentation du ministère selon laquelle il ne serait pas possible de limiter au strict nécessaire l'ingérence dans les droits reconnus aux articles 7 et 8 de la Charte ne saurait être admise.

En deuxième lieu, n'est pas limité au strict nécessaire un régime de

1. En effet, les points 66 et suivants de la décision *Digital Rights Ireland* ne concernent que l'absence de garanties nécessaires au regard de l'article 8 de la Charte et non de la limitation au strict nécessaire au regard de l'article 7. Seuls les points 57 à 65 de la décision concernent à la fois les critères de limitation au strict nécessaire au regard des articles 7 et 8 de la Charte.

conservation de données qui ne prévoit aucun critère objectif permettant de délimiter l'accès des autorités nationales compétentes aux données et leur utilisation ultérieure à des fins qui justifieraient l'ingérence dans les articles 7 et 8 de la Charte (point 60).

La Cour de justice a même précisé que ces fins doivent être « précises, strictement restreintes » (CJUE, g^{de} ch., 6 oct. 2015, *Schrems*, C-362/14, point 93 ; *voir aussi* CJUE, g^{de} ch., 8 avr. 2014, *Digital Rights Ireland*, C-293/12, C-594/12, points 60 et 61). Elle insiste par ailleurs sur la notion de contrôle indépendent de cet accès (point 62).

En troisième lieu, n'est pas non plus limité au strict nécessaire un régime de conservation de données « sans que soit opérée une quelconque distinction entre les catégories de données prévues [...] en fonction de leur utilité éventuelle aux fins de l'objectif poursuivi ou selon les personnes concernées » et « sans que soit précisée la détermination de la durée de conservation doit être fondée sur des critères objectifs afin de garantir que celle-ci est limitée au strict nécessaire. » (points 63 et 64)

Contrairement à ce qu'affirme le ministre, chacun de ces trois critères doit être respecté pour qu'un régime de conservation de données soit limité au strict nécessaire.

En effet, le respect d'un seul ou de seulement deux de ces trois critères ne saurait être de nature à pallier les manquements relevés par la Cour. Une telle analyse reviendrait, par exemple, à considérer à tort comme limité au strict nécessaire un régime de conservation qui se bornerait uniquement à prévoir une durée de conservation détérminée en fonction des objectifs et des personnes concernées (3^{e} critère), sans effectuer aucune limitation, différenciation ou exception au niveau de la conservation des données (1er critère) et sans limiter par des critères objectifs l'accès à ces données serait limité au strict nécessaire (2^{e} critère).

Or, une telle analyse serait contraire à la jurisprudence de la Cour de justice. La Cour de justice a clairement établi dans son arrêt *Schrems* que toute interprétation qui conduirait à considérer ces critères comme alternatifs serait contraire à la Charte :

> « 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 ***et*** 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 que comportent tant l'accès que l'utilisation de ces données. »
>
> (CJUE, g^{de} ch., 6 oct. 2015, *Schrems*, C-362/14, point 93)

Par conséquent, une lecture combinée de l'arrêt *Digital Rights Ireland* et de l'arrêt *Schrems* démontre sans équivoque que les trois critères exposés

précédemment doivent *tous* être respectés pour qu'un régime de conservation et d'accès aux données soit limité au strict nécessaire.

À défaut de quoi, transposée au cas d'espèce, la conclusion en droit ne saurait être différente de celle de la Cour de justice qui décida que :

> « Il résulte de ce qui précède que la directive 2006/24 ne prévoit 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. Force est donc de constater 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. »
> (CJUE, g^{de} ch., 8 avr. 2014, *Digital Rights Ireland*, C-293/12, C-594/12, point 65)

En l'espèce, pour les raisons déjà exposées par les associations requérantes dans leur mémoire complémentaire, le régime français ne réunit pas les conditions rappelées ci-dessus. Par conséquent, il n'est pas limité au strict nécessaire — ainsi que viennent le confirmer les développements suivants.

5. Sur l'absence de nécessité d'une conservation généralisée des données de connexion en raison de l'existence d'autres mesures au moins aussi efficaces

Pour que le principe de conservation généralisée des données puisse être jugé comme strictement nécessaire, encore faut-il que cette nécessité soit prouvée. Mais, à aucun moment de sa défense, le garde des sceaux n'apporte de justification à la conservation généralisée des données. À aucun moment il ne dit en quoi le système de conservation ciblée des données mis en place dans une majorité d'États européens n'est pas de nature à satisfaire l'objectif de prévention et de répression des crimes les plus graves.

Pourtant, comme l'énonce à raison l'avocat général Saugmandsgaard Øe dans ses conclusions du 19 juillet 2016 précitées :

> « Eu égard à l'exigence de stricte nécessité, il est impératif que ces juridictions ne se contentent pas de vérifier la simple utilité d'une obligation générale de conservation de données, mais vérifie strictement qu'aucune autre mesure ou combinaison de mesures, et notamment **une obligation ciblée de conservation de données accompagnée d'autres outils d'investigation**, ne peut offrir **la même efficacité dans la lutte contre les infractions graves**. Je souligne à cet égard que

> plusieurs études portées à l'attention de la Cour **remettent en cause la nécessité de ce type d'obligation aux fins de la lutte contre les infractions graves**. » (point 209)

À l'inverse, le garde des sceaux se confond dans l'affirmation selon laquelle, puisque des actes graves peuvent être commis par n'importe qui, toutes les données de connexion de l'ensemble de la population doivent être conservées. Or, cette affirmation ne saurait valoir démonstration. D'autant que, comme le rappelle l'avocat général, de nombreuses études témoignent à l'inverse de l'absence de nécessité d'une conservation généralisée des données de connextion (voir note de bas de page n° 65 des conclusions précitées du 19 juillet 2016).

6. Sur l'absence de garanties entourant l'accès aux données

Quant à l'encadrement des conditions d'accès aux données de connexion conservées, le garde des sceaux identifie trois conditions pouvant conduire à considérer que l'accès aux données de connexion est dûment encadré. Mais, à aucun moment, il ne justifie la conformité du droit français aux critères énoncés par la Cour de justice. Tout au plus affirme-t-il que «le système français dans le cadre du dispositif critiqué, offre des garanties suffisantes» (p. 10). Le fait que le ministre de la justice se cantonne à cette affirmation n'a rien de surprenant puisqu'aucune de ces trois conditions n'est satisfaite.

Premièrement, le ministre de la justice rappelle que la collecte doit être limitée aux cas de criminalité grave ou d'atteinte à la sécurité nationale. À ce sujet, il considère que les données recueillies sont utilisées essentiellement dans un cadre judiciaire et que l'accès administratif à ces données aurait été validé par le Conseil d'État. Mais, sur ce point, le ministre occulte les finalités déjà évoquées *supra* et associées aux articles L. 34-1 CPCE et 6 de la LCEN. Il occulte aussi l'utilisation, elle aussi évoquée *supra*, pouvant être faite des données de connexion notamment de par la lettre de l'article L. 851-1 du code de la sécurité intérieure en vue de l'accomplissement de la très large palette de finalités pouvant être poursuivies par les services de renseignement lorsqu'ils procèdent au recueil des données collectées.

Or, comme cela est démontré par les parties requérantes, ces finalités ne sont aucunement limitées à la criminalité grave mais sont au contraire largement indéterminées. Alors même que, comme cela a été rappelé par l'avocat général, « seule la lutte contre les infractions graves est susceptible de justifier une telle ingérence » (point 231).

Deuxièmement, un contrôle indépendant doit être effectué préalablement à l'accès aux données. Cela a encore été rappelé par l'avocat général Saugmandsgaard Øe :

> « l'accès aux données conservées doit être subordonné à un contrôle préalable effectué soit par une juridiction, soit par une entité

> administrative indépendante dont la décision vise à limiter l'accès aux données et leur utilisation à ce qui est strictement nécessaire aux fins d'atteindre l'objectif poursuivi. Ce contrôle préalable doit en outre intervenir à la suite d'une demande motivée de ces autorités présentée dans le cadre de procédures de prévention, de détection ou de poursuites pénales. » (point 232)

Mais quel contrôle par une juridiction ou une autorité administrative indépendante est organisé dans le système français ? Tout simplement aucun.

Tout au plus les articles L. 821-1 et L. 851-1 du code de la sécurité intérieure donnent-ils à la Commission nationale de contrôle des techniques de renseignement (CNCTR) un pouvoir d'avis lorsque les services désignés souhaitent accéder aux données de connexion. Mais ce pouvoir d'avis, non contraignant, ne remplit pas la condition de l'avocat général Saugmandsgaard Øe, qui parle de *décision* devant être adoptée par une autorité administrative indépendante. Ce qui n'est encore une fois pas du tout le cas de la CNCTR.

Troisièmement, les données recueillies par les autorités doivent être protégées dans leur utilisation ultérieure. A ce sujet, le ministre rappelle bien que «le droit national doit limiter au strict nécessaire le nombre de personnes qui disposent de l'autorisation d'accès et d'utilisation ultérieure des données conservées». Or, en droit français, l'accès à ces données, une fois obtenues auprès des fournisseurs d'accès à internet et hébergeurs, n'est encadré d'aucune manière que ce soit. Il est donc faux de dire, comme le fait le ministre, que le «droit français limite au strict nécessaire le nombre de personnes qui disposent de l'autorisation d'accès et d'utilisation ultérieure des données conservées.»

En somme, l'absence de démonstration du garde des sceaux de la satisfaction des conditions d'accès telles que définies par la Cour a pour seule cause l'absence de respect par le droit français de ces conditions.

7. Sur le pêle-mêle final du ministre sur « le caractère proportionné à l'objectif de l'ingérence »

Dans une partie finale sur le « caractère proportionné à l'objectif de l'ingérence » (pp. 12 et s.), on retrouve pêle-mêle une série d'arguments portant sur le soit-disant caractère proportionné à l'objectif de l'ingérence. Ces éléments seraient étonnants s'ils ne faisaient pas que témoigner avec gravité de l'incapacité du ministre à défendre le système en place. Avant d'aborder une série de trois considérations devant être contredites, le ministre de l'intérieur évoque de manière préliminaire trois points qui, eux aussi, devront être contredits.

Tout d'abord, comme à court d'arguments, le garde des sceaux justifie

d'abord la collecte généralisée des données en se fondant sur l'arrêt *Marper*[2], lequel ne fait référence qu'à un « traitement automatique » de certaines données et aucunement à une conservation généralisée des données de connexion.

Ensuite, le ministre cite une recommandation du Conseil de l'Europe dans laquelle il est fait référence au fait que la collecte de données à caractère personnel « devrait se limiter à ce qui est nécessaire à la prévention d'un danger concret ou à la répression d'une infraction pénale déterminée ». Ce qui ne fait qu'ajouter à l'argumentation des requérantes. D'une part, le Gouvernement n'a jamais pu démontrer en quoi la conservation des données devait être limitée à ce qui est nécessaire. D'autre part, les articles 6, II, de la loi du 21 juin 2004, L. 34-1 CPCE et L. 851-1 du code de la sécurité intérieure ne limitent en rien le dispositif attaqué « à ce qui est nécessaire à la prévention d'un danger concret ou à la répression d'une infraction pénale déterminée ». Au contraire, comme cela a déjà été démontré à de nombreuses reprises par les requérantes, ces articles ouvrent de manière extrêmement large le champ des finalités de la collecte, auxquelles viennent s'ajouter celles encore plus larges issues de la loi renseignement.

Enfin, le ministre semble induire que la mise en cause de données de connexion (ou métadonnées) serait moins attentatoire aux libertés que ne le serait celle de données de contenu. Sur ce point l'avocat général Saugmandsgaard Øe rappelle bien, à l'instar de l'avocat général Cruz Villalon, que la conservation généralisée des données de connexion emporte de graves risques qui « n'ont rien de théorique » (point 260 des conclusions du 19 juillet 2016 précitées) pour la société dans son ensemble.

Car, « à la différence de mesures de surveillance ciblées, une telle obligation est susceptible de faciliter considérablement les ingérences de masse, c'est-à-dire les ingérences affectant une partie substantielle ou même l'ensemble de la population pertinente » (point 256 des conclusions du 19 juillet 2016). Et l'avocat général d'illustrer aux points 257 et s. la gravité des atteintes pouvant naître d'une conservation généralisée des données. En ce sens, l'avocat général Saugmandsgaard Øe souligne encore dans ses conclusions du 19 juillet 2016 que « les risques liés à l'accès aux données relatives aux communications (ou « métadonnées ») peuvent être équivalents, voire supérieurs à ceux résultant de l'accès au contenu de ces communications » (point 259).

7.1. Sur les garanties de l'article L. 34-1 CPCE

Pas plus qu'auparavant, le ministre ne peut démontrer ici en quoi le régime en place répondrait aux limitations imposées par la Cour de justice et n'amorce d'ailleurs pas même l'once d'une démonstration. Au contraire, il tisse frauduleusement une lecture éronnée de l'article L. 34-1 CPCE en affirmant que cet article se limite aux « infractions graves ou d'atteintes à la sécurité nationale » (p. 13) là où l'article est ouvert au contraire à la

2. Cour EDH, g^de^ ch., 4 déc. 2008, *Marper c. R-U*, n^os^ 30562/04 et 30566/04

recherche, à la contestation et à la poursuite « des infractions pénales ». Sans oublier les atteintes au droit d'auteur, dont on peine à savoir si elles relèvent des infractions graves ou de la sécurité nationale.

Le ministre oublie aussi, fait maintes fois rappelé par les associations requérantes, que la réquisition des données par l'autorité judiciaire peut se faire sur n'importe quel motif et dans le cadre de n'importe quelle affaire. En rien, il ne s'agit pour le juge d'être limité à la commission de crimes graves ou d'atteintes à la sécurité nationale. L'article 6, II ne fait que disposer à cet effet que « L'autorité judiciaire peut requérir communication auprès des prestataires mentionnés aux 1 et 2 du I des données mentionnées au premier alinéa. »

Et nul besoin là encore d'insister une fois de plus sur le fait que le ministre ignore totalement les finalités extrêmement larges de la loi renseignement ainsi que l'absence dans ce cadre de tout contrôle indépendant à l'accès aux données collectées.

7.2. Sur la durée de conservation des données

Le garde des sceaux tente alors vainement de « compenser » (p. 14) les défaillances inhérentes au système de conservation généralisée des données de connexion en tentant de justifier d'une durée de conservation d'un an, voire plus. Mais pour ce faire, le ministre s'appuie de manière pour le moins surprenante, sur une délibération de la CNIL selon laquelle « un délai de conservation de trois mois est suffisant pour l'essentiel des usages qu'elles peuvent avoir ». Car il est en effet bien certain qu'une durée de conservation excédant six mois est proprement inutile comme en témoignent les illustrations étrangères et notamment européennes.

En ce sens, l'avocat général Saugmandsgaard Øe rappelle la jurisprudence de la Cour EDH [3] et souligne dans ses conclusions du 19 juillet 2016 précitées que « la Cour EDH, dans le récent arrêt Roman Zakharov c. Russie, a jugé raisonnable une durée maximale de conservation de six mois, tout en déplorant l'absence d'obligation de détruire sur le champ les données qui n'ont pas de rapport avec le but pour lequel elles ont été recueillies » (point 243). Et l'avocat général a d'ailleurs raison de souligner au même point de ses conclusions l'obligation de destruction des données collectées qui n'est aucunement prévue en droit français.

7.3. Sur la protection des données collectées

Pour conclure son mémoire en défense, le ministre considère que l'obligation générale faite aux opérateurs et hébergeurs de sécuriser les données personnelles qu'ils stockent dans le cadre de leurs activités suffit à garantir la sécurité des données qu'ils sont tenus de conserver. Mais la défosse de l'État ne saurait suffire. En quoi une obligation générale de sécurisation

3. Cour EDH, g^{de} ch., 4 déc. 2015, *Zakharov c. Russie*, n^{o} 47143/06

pourrait garantir la sécurité des données ? En rien, comme le démontrent les nombreuses fuites dont font l'objet de telles données de manière régulière.

D'ailleurs, l'avocat général Saugmandsgaard Øe rappelle que les États doivent « garantir le contrôle par une autorité indépendante, exigé par l'article 8, paragraphe 3, de la Charte, du respect des exigences de protection et de sécurité énoncées aux points 66 et 67 » de l'arrêt *Digital Rights Ireland* (point 238). Ce que le système français n'encadre en rien.

7.4. Sur la proportionnalité *stricto sensu* de la conservation généralisée des données

Enfin, il est remarquable que le ministre, dans une partie de son mémoire en défense dédié à la proportionnalité des mesures en cause, n'ait pas même pris le soin de démontrer en quoi la conservation généralisée des données procédait d'un arbitrage raisonné entre l'atteinte faite aux droits et libertés d'une part et la protection de la sécurité naitonale d'autre part.

La situation à laquelle nous faisons face est celle d'un État qui, dans la perspective légitime de protéger sa population, déploie un arsenal de mesures inefficaces en plus d'être attentatoires aux libertés. Dans cette situation de déraison, les parties requérantes ne peuvent alors que s'en remettre au juge de l'excès de pouvoir afin qu'il exige de l'administration nationale qu'elle justifie ses choix. Car lui seul est en mesure, en plus d'être dans l'obligation, de le faire.

Et le caractère impérieux d'une telle demande est désormais bien avéré. Comme cela a été très clairement relevé par l'avocat général Saugmandsgaard Øe dans ses conclusions précitées du 19 juillet 2016 :

> « À la différence des exigences relatives au caractère approprié et nécessaire de la mesure en cause, lesquelles évaluent son efficacité au regard de l'objectif poursuivi, l'exigence de proportionnalité stricto sensu consiste à mettre en balance, d'une part, les avantages résultant de cette mesure au regard de l'objectif légitime poursuivi avec, d'autre part, les inconvénients en découlant au regard des droits fondamentaux consacrés dans une société démocratique. **Cette exigence ouvre ainsi un débat sur les valeurs devant prévaloir dans une société démocratique et, en définitive, sur le type de société dans lequel nous souhaitons vivre.** » (point 248)

C'est à l'aune de cette considération, qu'en l'état du droit, le juge national doit, d'après les termes de l'avocat général « apprécier si les inconvénients causés par les obligations générales de conservation de données en cause dans les litiges au principal ne sont pas démesurés, dans une société démocratique, par rapport aux buts visés » (point 261 des conclusions du 19 juillet 2016 précitées).

Par ces motifs, et tous autres à produire, déduire, suppléer, au besoin même d'office, les exposantes persistent dans les conclusions de leurs précédentes écritures.

Le 22 juillet 2016, 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

TABLE DES JURISPRUDENCES ET CONCLUSIONS