Fédération FDN
16, rue de Cachy
80 090 Amiens
W751210904

La Quadrature du Net
60, rue des Orteaux
75 020 Paris
W751218406

French Data Network
16, rue de Cachy
80 090 Amiens
W751107563

Demande d'abrogation de dispositions réglementaires

Paris, le 27 avril 2015

Monsieur le Premier ministre,

Objet : demande d'abrogation de l'article R. 10-13 CPCE et du 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

Copie : Ministère de l'intérieur, Ministère de la défense, Ministère de la justice, Ministère de l'industrie, Secrétariat d'État au numérique.

1 Dispositions dont l'abrogation est demandée

Par la présente, les associations demandent au gouvernement d'abroger l'article R. 10-13 du code des postes et des télécommunications (CPCE), qui définit les données que les fournisseurs d'accès à Internet (FAI) ont obligation de conserver de par l'article L. 34-1 du CPCE, et du 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), pris en application de l'article 6-II bis de la loi n° 2004-575 du 21 juin 2004 sur la confiance dans l'économie numérique.

1.1 Article R. 10-13 du CPCE

L'article R. 10-13 CPCE a été pris en application de l'article L. 34-1 III CPCE. Ce dernier article autorise les opérateurs de communications électroniques à différer d'un an l'effacement de certaines données techniques relatives à leurs abonnés, par dérogation à l'obligation prévue à l'article L. 34-1 II CPCE de les effacer ou de les rendre anonymes immédiatement.

L'article L. 34-1 CPCE prévoit en effet que :

> *« II.-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.

[...]

« III.-Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales ou d'un manquement à l'obligation définie à l'article L. 336-3 du code de la propriété intellectuelle ou pour les besoins de la prévention des atteintes aux systèmes de traitement automatisé de données prévues et réprimées par les articles 323-1 à 323-3-1 du code pénal, et dans le seul but de permettre, en tant que de besoin, la mise à disposition de l'autorité judiciaire ou de la haute autorité mentionnée à l'article L. 331-12 du code de la propriété intellectuelle ou de l'autorité nationale de sécurité des systèmes d'information mentionnée à l'article L. 2321-1 du code de la défense, ***il peut être différé*** *pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques. Un décret en Conseil d'État, 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'État, par les opérateurs. »*

En effet, l'article R. 10-13 CPCE dispose :

« 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. »

1.2 Décret n° 2011-219 du 25 février 2011

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

« I.-1. Les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne [...]

« 2. Les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services [...]

« II.- 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.*

[...]

« Un décret en Conseil d'État, 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 n° 2011-219, pris en application de cet article 6 II de la LCEN, prévoit au point 1° de son premier article l'obligation pour les fournisseurs d'accès à Internet de conserver une liste de données permettant d'identifier leurs abonnés à chacune de leur connexion :

« Les données mentionnées au II de l'article 6 de la loi du 21 juin 2004 susvisée, que les personnes sont tenues de conserver en vertu de cette disposition, sont les suivantes :

« 1° Pour les personnes mentionnées au 1 du I du même article et pour chaque connexion de leurs abonnés :

a) L'identifiant de la connexion ;

b) L'identifiant attribué par ces personnes à l'abonné ;

c) L'identifiant du terminal utilisé pour la connexion lorsqu'elles y ont accès ;

d) Les dates et heure de début et de fin de la connexion ;

e) Les caractéristiques de la ligne de l'abonné ;

« 2° Pour les personnes mentionnées au 2 du I du même article et pour chaque opération de création :

a) L'identifiant de la connexion à l'origine de la communication ;

b) L'identifiant attribué par le système d'information au contenu, objet de l'opération ;

c) Les types de protocoles utilisés pour la connexion au service et pour le transfert des contenus ;

d) La nature de l'opération ;

e) Les date et heure de l'opération ;

f) L'identifiant utilisé par l'auteur de l'opération lorsque celui-ci l'a fourni ;

« 3° Pour les personnes mentionnées aux 1 et 2 du I du même article, les informations fournies lors de la souscription d'un contrat par un utilisateur ou lors de la création d'un compte :

a) Au moment de la création du compte, l'identifiant de cette connexion ;
b) Les nom et prénom ou la raison sociale ;
c) Les adresses postales associées ;
d) Les pseudonymes utilisés ;
e) Les adresses de courrier électronique ou de compte associées ;
f) Les numéros de téléphone ;
g) Le mot de passe ainsi que les données permettant de le vérifier ou de le modifier, dans leur dernière version mise à jour ;

« 4° Pour les personnes mentionnées aux 1 et 2 du I du même article, lorsque la souscription du contrat ou du compte est payante, les informations suivantes relatives au paiement, pour chaque opération de paiement :

a) Le type de paiement utilisé ;
b) La référence du paiement ;
c) Le montant ;
d) La date et l'heure de la transaction. »

2 Changement de circonstance postérieure à l'adoption de ces dispositions : l'arrêt *Digital Rights* de la CJUE

La demande d'abrogation de ces dispositions résulte du changement de circonstance en droit de l'Union européenne résultant de l'arrêt rendu par la Cour de justice de l'Union européenne dans son arrêt du 8 avril 2014, l'arrêt *Digital Rights Ireland*, C-293/12. Dans cette décision, la grande chambre de la CJUE a invalidé la directive 2006/24/CE relative à la conservation des données par les opérateurs de communications électroniques, la jugeant non conforme à la Charte des droits fondamentaux de l'Union européenne (la Charte).

S'agissant d'Internet, la directive imposait aux fournisseurs d'accès à Internet de conserver pour une durée de six mois à deux ans :

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

i) le(s) numéro(s) d'identifiant attribué(s) ;
ii) le numéro d'identifiant et le numéro de téléphone attribués à toute communication entrant dans le réseau téléphonique public ;

iii) les nom et adresse de l'abonné ou de l'utilisateur inscrit à qui une adresse IP (protocole internet), un numéro d'identifiant ou un numéro de téléphone a été attribué au moment de la communication ;

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

i) le numéro d'identifiant ou le numéro de téléphone du (des) destinataire(s) prévu(s) d'un appel téléphonique par l'internet ;

ii) les nom et adresse de l'abonné (des abonnés) ou de l'utilisateur (des utilisateurs) inscrit(s) et le numéro d'identifiant du destinataire prévu de la communication ;

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

i) la date et l'heure de l'ouverture et de la fermeture de la session du service d'accès à l'internet dans un fuseau horaire déterminé, ainsi que l'adresse IP (protocole internet), qu'elle soit dynamique ou statique, attribuée à une communication par le fournisseur d'accès à l'internet, ainsi que le numéro d'identifiant de l'abonné ou de l'utilisateur inscrit ;

ii) la date et l'heure de l'ouverture et de la fermeture de la session du service de courrier électronique par l'internet ou de téléphonie par l'internet dans un fuseau horaire déterminé ;

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

i) le service internet utilisé ;

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

i) le numéro de téléphone [IP] de l'appelant pour l'accès commuté ;

ii) la ligne d'abonné numérique (DSL) ou tout autre point terminal de l'auteur de la communication ;

« f) les données nécessaires pour localiser le matériel de communication mobile :

i) les données permettant d'établir la localisation géographique des cellules, en se référant à leur identité de localisation (identifiant cellulaire), pendant la période au cours de laquelle les données de communication sont conservées.

2.1 Le champ trop large des personnes et des données visées

Pour déclarer cette directive invalide, la CJUE a d'abord estimé que l'obligation généralisée de conservation des données de connexion ainsi que l'accès qui en était donné aux autorités nationales constituaient des ingérences dans les droits fondamentaux au respect de la vie privée et familiale et à la protection des données à caractère personnel reconnus aux articles 7 et 8 de la Charte. Comme l'a décidé la CJUE :

« (...) 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. » (§ 58)*

« (...)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. » (§ 59)

2.2 L'absence de limitation du champ des infractions concernées

La Cour invalide également la directive en constatant l'absence de limitation précise du champ des infractions pouvant justifier la conservation des données visées. Selon la Cour :

« (...) L'article 4 de cette directive, qui régit l'accès de ces autorités aux données conservées, ne dispose pas expressément que cet accès et l'utilisation ultérieure des données en cause doivent être strictement restreints à des fins de prévention et de détection d'infractions graves précisément délimitées ou de poursuites pénales afférentes à celles-ci. » (§ 61)

2.3 L'absence de distinction des différents types de données

L'un des autres griefs de la Cour à l'encontre de la directive concerne l'application d'un régime équivalent pour des types de données variés dont la conservation doit s'analyser comme représentant différents niveaux d'ingérence dans le droit à la vie privée. D'après la Cour :

« (...) s'agissant de la durée de conservation des données, la directive 2006/24 impose, à son article 6, la conservation de celles-ci pendant une période d'au moins six mois sans que soit opérée une quelconque distinction entre les catégories de données prévues à l'article 5 de cette directive en fonction de leur utilité

éventuelle aux fins de l'objectif poursuivi ou selon les personnes concernées. » (§ 63)

2.4 Droit applicable du fait de l'invalidation de la directive de 2006

Suite à l'invalidation de la directive 2006/24, le droit de l'Union européenne applicable est désormais celui qui résulte de la 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 dite « ePrivacy »). Cette directive dispose dans son article 15 que :

> *« Les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue* ***une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique****, pour sauvegarder la sécurité nationale — c'est-à-dire la sûreté de l'État — la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe. Toutes les mesures visées dans le présent paragraphe sont prises dans le respect des principes généraux du droit communautaire, y compris ceux visés à l'article 6, paragraphes 1 et 2, du traité sur l'Union européenne. »*

Lu à la lumière de l'arrêt du 8 avril 2014 rendu par la CJUE, et en particulier de ses paragraphes 57 à 59, l'article 15 de la directive 2002/58/CE tend à invalider le principe même d'une obligation de conservation des données pour les 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 »*, pour privilégier des dispositifs de conservation de données ciblées, tant en termes temporels que s'agissant des personnes concernées (conservation sur injonction).

2.5 Conséquences du changement de circonstance dans les autres États membres

Dans de nombreux États membres de l'Union Européenne, l'arrêt *Digital Rights* a des répercussions importantes sur le droit applicable pour les régimes d'accès administratifs

et judiciaires aux données détenues par les fournisseurs d'accès à Internet et par les hébergeurs.

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 « un-selecteve » 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.

Enfin, aux Pays-Bas, la loi néerlandaise imposait une conservation des données pour une durée de 6 à 12 mois. 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.

3 Applicabilité du changement de circonstance aux dispositions réglementaires visées

La jurisprudence *Digital Rights* doit conduire le gouvernement français à abroger les dispositions réglementaires susvisées.

En effet, tant l'article R. 10-13 du CPCE que le décret n° 2011-219 du 25 février 2011 violent la Charte des droits fondamentaux de l'Union européenne et la directive *ePrivacy* de 2002.

Ces dispositions françaises afférentes au régime de conservation des données ont un champ d'application bien trop large, puisqu'elles portent atteinte à la vie privée de 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 ». Elles ne prévoient d'ailleurs aucune exception pour les personnes dont les communications sont soumises au secret professionnel, tels que les journalistes ou les avocats. Leur application n'est pas non plus limitée aux données afférentes à une période

temporelle et/ou une zone géographique déterminée. Elles ne prévoient pas non plus de limites quant aux infractions justifiant l'accès aux données conservées. Elles créent au demeurant un régime homogène, notamment s'agissant de la durée de conservation, sans considération de leur utilité éventuelle aux fins de l'objectif.

Enfin, l'ingérence dans le droit à la vie privée qui résulte de ces dispositions est plus importante que celle instituée par la directive de 2006 invalidée. En effet, le champ des données conservées était bien plus restreint s'agissant de cette dernière.

En conlusion, pour respecter le droit à la vie privée et le principe de proportionalité prévus par la Charte des droits fondamentaux telle qu'interprétée par la CJUE, les dispositions réglementaires suvisées doivent être abrogées.

Souhaitant vous voir agir au plus vite, veuillez accepter M. le Premier ministre, l'expression de notre considération distinguée.

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

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

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