Conseil d'État
Section du contentieux

Requête introductive d'instance

introduite

PAR

1. **French Data Network (Réseau de données français)**, dite FDN.
   Association régie par la loi du 1er juillet 1901 établie 16 rue de Cachy, 80090 Amiens, enregistrée en préfecture de la Somme sous le numéro W751107563, opérateur déclaré auprès de l'ARCEP sous la référence 07/1149, prise en la personne de son président M. Fabien Sirjean.
   Tel. : 06 36 18 91 00
   Mail : `president@fdn.fr` / `buro@fdn.fr`
2. **La Quadrature du Net**, dite LQDN
   Association régie par la loi du 1er juillet 1901 établie au 60 rue des Orteaux, 75020 Paris, enregistrée en préfecture de police de Paris sous le numéro W751218406, prise en la personne de son président M. Philippe Aigrain.
   Tel. : 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.
   Tel. : 06 60 24 24 94
   Mail : `contact@ffdn.org`

CONTRE

Le décret nº 2015-125 du 5 février 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique, publié au JORF nº 31 du 6 février 2015, page 1811

0. Table des matières

1 FAITS **3**

1.1 La décision attaquée 3

1.2 Les notions employées dans le décret 5

1.2.1 Notions de nom de domaine, de nom d'hôte, de DNS et de nom de serveur 5

1.2.2 Notion d'adresse électronique d'un service de communication au public en ligne 6

1.2.3 Techniques de blocages possibles 7

2 DISCUSSION — Intérêt à agir **9**

2.1 French Data Network 9

2.2 La Quadrature du Net 9

2.3 Fédération des fournisseurs d'accès à Internet associatifs 11

3 DISCUSSION — Légalité externe **12**

3.1 Incompétences 12

3.1.1 Le décret attaqué porte une atteinte à la liberté de communication non prévue par la loi 12

3.1.2 Le décret porte une atteinte au secret des correspondances non prévue par la loi 14

3.2 Vices de procédure 16

3.2.1 Absence d'arrêté autorisant le traitement de données à caractère personnel par l'administration 16

3.2.2 Absence d'étude d'impact antérieure au décret 17

4 DISCUSSION — Légalité interne **18**

4.1 Le décret viole la séparation des pouvoirs 18

4.2 Le décret n'est ni clair, ni intelligible 21

4.3 Le blocage de sites porte une atteinte disproportionnée à la liberté d'expression 23
4.3.1 Les mesures de blocage de sites sont inefficaces 23
4.3.2 Les mesures de blocage impliquent d'importants effets collatéraux 27
4.3.3 Il existe des mesures efficaces alternatives au blocage 30
4.4 L'absence de contrôle juridictionnel viole les droits fondamentaux 34
4.4.1 La loi et le décret ne réunissent pas les garanties suffisantes pour éviter les abus 34
4.4.2 Les voies de recours a posteriori sont ineffectives 37
4.4.3 Le contrôle des mesures par une personne qualifiée de la CNIL est ineffectif 40
4.5 L'interception des communications vers les sites bloqués est illégale . . . 40
4.5.1 Le transfert de données que constitue la redirection depuis les services bloqués est illégal 41
4.5.2 La collecte de données résultant de la redirection depuis les services bloqués est illégale 42
4.5.3 La redirection depuis les services bloqués porte une atteinte disproportionnée aux droits et libertés fondamentaux 43

1. FAITS

1.1. La décision attaquée

Le 14 mars 2011, le Parlement adoptait la loi d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI). Par son article 4, cette loi modifiait l'article 6, I, de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) en y insérant les deux alinéas suivants :

> *« Lorsque les nécessités de la lutte contre la diffusion des images ou des représentations de mineurs relevant de l'article 227-23 du code pénal le justifient, l'autorité administrative notifie aux personnes mentionnées au 1 du présent I les adresses électroniques des services de communication au public en ligne contrevenant aux dispositions de cet article, auxquelles ces personnes doivent empêcher l'accès sans délai.*
> *« Un décret fixe les modalités d'application de l'alinéa précédent, notamment celles selon lesquelles sont compensés, s'il y a lieu, les surcoûts résultant des obligations mises à la charge des opérateurs. »*

Pour rappel, l'article 227-23 du code pénal susvisé dispose que :

> *« Le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende.*
> *« Le fait d'offrir, de rendre disponible ou de diffuser une telle image ou représentation, par quelque moyen que ce soit, de l'importer ou de l'exporter, de la faire importer ou de la faire exporter, est puni des mêmes peines.*
> *« Les peines sont portées à sept ans d'emprisonnement et à 100 000 euros d'amende lorsqu'il a été utilisé, pour la diffusion de l'image ou de la représentation du mineur à destination d'un public non déterminé, un réseau de communications électroniques.*
> *« La tentative des délits prévus aux alinéas précédents est punie des mêmes peines.*
> *« Le fait de consulter habituellement un service de communication au public en ligne mettant à disposition une telle image ou représentation ou de détenir une telle image ou représentation par quelque moyen que ce soit est puni de deux ans d'emprisonnement et 30 000 euros d'amende.*

« Les infractions prévues au présent article sont punies de dix ans d'emprisonnement et de 500 000 euros d'amende lorsqu'elles sont commises en bande organisée.

« Les dispositions du présent article sont également applicables aux images pornographiques d'une personne dont l'aspect physique est celui d'un mineur, sauf s'il est établi que cette personne était âgée de dix-huit ans au jour de la fixation ou de l'enregistrement de son image. »

Le 13 novembre 2014, le Parlement adoptait la loi n° 2014-1353 renforçant les dispositions relatives à la lutte contre le terrorisme. Son article 12 modifie la LCEN en y insérant un nouvel article 6-1 :

« Lorsque les nécessités de la lutte contre la provocation à des actes terroristes ou l'apologie de tels actes relevant de l'article 421-2-5 du code pénal ou contre la diffusion des images ou des représentations de mineurs relevant de l'article 227-23 du même code le justifient, l'autorité administrative peut demander à toute personne mentionnée au III de l'article 6 de la présente loi ou aux personnes mentionnées au 2 du I du même article 6 de retirer les contenus qui contreviennent à ces mêmes articles 421-2-5 et 227-23. Elle en informe simultanément les personnes mentionnées au 1 du I de l'article 6 de la présente loi.

« En l'absence de retrait de ces contenus dans un délai de vingt-quatre heures, l'autorité administrative peut notifier aux personnes mentionnées au même 1 la liste des adresses électroniques des services de communication au public en ligne contrevenant auxdits articles 421-2-5 et 227-23. Ces personnes doivent alors empêcher sans délai l'accès à ces adresses. Toutefois, en l'absence de mise à disposition par la personne mentionnée au III du même article 6 des informations mentionnées à ce même III, l'autorité administrative peut procéder à la notification prévue à la première phrase du présent alinéa sans avoir préalablement demandé le retrait des contenus dans les conditions prévues à la première phrase du premier alinéa du présent article.

« L'autorité administrative transmet les demandes de retrait et la liste mentionnées, respectivement, aux premier et deuxième alinéas à une personnalité qualifiée, désignée en son sein par la Commission nationale de l'informatique et des libertés pour la durée de son mandat dans cette commission. Elle ne peut être désignée parmi les personnes mentionnées au 1° du I de l'article 13 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. La personnalité qualifiée s'assure de la régularité des demandes de retrait et des conditions d'établissement, de mise à jour, de communication et d'utilisation de la liste. Si elle constate une irrégularité, elle peut à tout moment recommander à l'autorité administrative d'y mettre fin. Si l'autorité administrative ne suit pas cette recommandation, la personnalité qualifiée peut saisir la juridiction administrative compétente, en référé ou sur requête.

« L'autorité administrative peut également notifier les adresses électroniques dont les contenus contreviennent aux articles 421-2-5 et 227-23 du code pénal aux moteurs de recherche ou aux annuaires, lesquels prennent toute mesure utile destinée à faire cesser le référencement du service de communication au public en ligne. La procédure prévue au troisième alinéa du présent article est applicable.

« La personnalité qualifiée mentionnée au même troisième alinéa rend public chaque année un rapport d'activité sur les conditions d'exercice et les résultats de son

activité, qui précise notamment le nombre de demandes de retrait, le nombre de contenus qui ont été retirés, les motifs de retrait et le nombre de recommandations faites à l'autorité administrative. Ce rapport est remis au Gouvernement et au Parlement.

« Les modalités d'application du présent article sont précisées par décret, notamment la compensation, le cas échéant, des surcoûts justifiés résultant des obligations mises à la charge des opérateurs.

« Tout manquement aux obligations définies au présent article est puni des peines prévues au 1 du VI de l'article 6 de la présente loi. »

L'article 5 de cette loi du 13 novembre 2014 créait aussi l'article 421-2-5 du code pénal, lequel dispose que :

« Le fait de provoquer directement à des actes de terrorisme ou de faire publiquement l'apologie de ces actes est puni de cinq ans d'emprisonnement et de 75 000 € d'amende.

« Les peines sont portées à sept ans d'emprisonnement et à 100 000 € d'amende lorsque les faits ont été commis en utilisant un service de communication au public en ligne.

« Lorsque les faits sont commis par la voie de la presse écrite ou audiovisuelle ou de la communication au public en ligne, les dispositions particulières des lois qui régissent ces matières sont applicables en ce qui concerne la détermination des personnes responsables. »

L'adoption des lois du 14 mars 2011 et du 13 novembre 2014 a été suivie par l'adoption du décret n° 2015-125 du 5 février 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique.

C'est la décision attaquée.

1.2. Les notions employées dans le décret

Le présent décret utilise plusieurs notions inédites en droit qu'il convient d'expliciter techniquement afin de pouvoir ensuite en tirer les conséquences juridiques.

1.2.1. Notions de nom de domaine, de nom d'hôte, de DNS et de nom de serveur

Au troisième alinéa de son article 2, le présent décret utilise les notions inédites en droit de « nom d'hôte » et de « nom de serveur » :

« Les adresses électroniques figurant sur la liste comportent soit un nom de domaine (DNS), soit un nom d'hôte caractérisé par un nom de domaine précédé d'un nom de serveur. »

Techniquement, un hôte est toute machine connectée à un réseau, soit qu'elle propose des contenus ou services, soit qu'elle utilise ces contenus ou services, soit qu'elle fasse les deux. Accéder à un hôte demande de connaître son adresse numérique sur le réseau (adresse IP, par exemple). Pour des raisons pratiques, il est possible d'associer à cette adresse numérique un nom, plus simple à utiliser, qu'on appelle « nom d'hôte ».

Certains noms d'hôte sont enregistrés sur des annuaires publics (appelés serveurs DNS) afin que chacun puisse les utiliser pour accéder aux adresses IP des hôtes auxquels les noms sont associés. Un nom d'hôte ainsi enregistré sur un serveur DNS est appelé « nom de domaine ». Il existe des noms de domaines courts (`monsite.fr`), ou d'autres plus longs ou plus compliqués (`www.impots.gouv.fr`).

La formulation utilisée par le décret « nom de domaine précédé d'un nom de serveur », soit n'a pas de sens, soit fait référence à des dénominations commerciales : le nom de domaine serait le produit acheté (`mon-domaine.com`) et le nom d'hôte serait ce que l'utilisateur a pu placer devant (`www.mon-domaine.com` ou `client.intranet.mon-domaine.com`).

Le décret opère une confusion sémantique à plusieurs niveaux, qu'il nous faut différencier clairement :

- la notion de nom de domaine, au sens commercial du terme : un nom vendu, loué ou offert, sous une racine donnée, par exemple `exemple.fr` sous la racine `.fr`, ou `exemple.co.uk` sous la racine `.co.uk` ou `exemple.fr.eu.org` pour la branche française de la racine `.eu.org` (`eu.org` étant lui même un domaine, vendu par la racine `.org` à l'association qui le gère) ;
- la notion de nom de domaine complet (*fully qualified domain name*, en anglais) qui désigne le nom complet d'un système, quelle que soit sa construction ; l'approche décrite par le décret (un nom local suivi d'un nom de domaine) correspond à l'usage habituel dans un réseau de bureautique ;
- la notion de DNS, qui techniquement désigne un annuaire public permettant de traduire un nom de domaine en une adresse numérique, est confondue avec la notion de nom de domaine (qui est un nom d'hôte inconnu localement et restant à traduire en adresse numérique).

La notion de « *nom de serveur* », bien qu'utilisée dans le décret est, quant à elle, trop floue pour être rattachée à une notion technique précise.

En faisant abstraction de cette confusion du décret, on peut légitimement supposer que la formule « nom de domaine précédé d'un nom de serveur » désigne en réalité un « nom de domaine ». L'article 2 alinéa 3 du décret signifie donc que « les adresses électroniques figurant sur la liste comportent [un nom de domaine] ».

1.2.2. Notion d'adresse électronique d'un service de communication au public en ligne

En droit, la notion de « *service de communication au public en ligne* » désigne toute forme de publication de contenu en ligne, quel que soit le protocole utilisé à cette fin : site Web (qu'il s'agisse d'héberger ou d'éditer un site), diffusion de vidéo (en direct comme en différé), bases de données (horaires de chemins de fer, état du trafic routier), service d'archivage d'informations, etc.

Le décret attaqué reprend la formule inédite du législateur d'« *adresses électroniques des services de communication au public en ligne* ». Le décret précise, à son article 2, que les « adresses électroniques figurant sur la liste **comportent** [un nom de domaine] » : l'adresse électronique est donc caractérisée par l'inclusion au minimum d'un nom de domaine.

Cette notion recouvre donc trois situations techniques distinctes :

1. L'adresse d'une page Web précise, alors appelée « adresse URL » (pour « Uniform resource locator »), par exemple :
   `http://monsite.fr/fichier.html`
2. Un nom de domaine sur un protocole précis, par exemple quant au protocole Web :
   `http://monsite.fr`
3. Un nom de domaine, sans autre précision sur le protocole ou le service visé, par exemple :
   `monsite.fr`

Le problème que pose la confusion terminologique dans la rédaction du décret apparaît lorsque l'on envisage les différentes techniques de blocage susceptibles d'être mises en œuvre.

1.2.3. Techniques de blocages possibles

La mesure de blocage de chacune de ces « adresses électroniques » entraîne des problèmes techniques spécifiques, ainsi que des coûts particuliers pour les opérateurs.

Blocage par URL Le blocage par URL suppose d'intercepter toutes les communications à destination du système fournissant le service de communication au public en ligne, puis d'analyser chaque requête en temps réel pour déterminer lesquelles portent sur la ou les adresses bloquées, et de remplacer à la volée ces requêtes et les réponses associées par la page d'information du ministère de l'intérieur prévue par le décret.

L'interception pose deux problèmes majeurs. D'une part, il faut placer en cœur de réseau des dispositifs capables de rediriger les flux à destination des services pour l'outil d'analyse, ce qui demande donc un aménagement notable du réseau de l'opérateur. D'autre part, ces communications peuvent être chiffrées, et donc inaccessibles au fournisseur d'accès à Internet.

L'interception de communications chiffrées ne peut se faire qu'avec des techniques plus lourdes, le système mis en œuvre se faisant passer pour le site demandé par l'utilisateur, proposant de fausses clefs de chiffrement et réalisant ainsi une attaque informatique connue sous le nom de *man in the middle*[1]. La majorité des logiciels modernes détectent ces attaques et les signalent aux utilisateurs. Il serait donc nécessaire, de surcroît, de prévoir une coopération des éditeurs de logiciels pour qu'ils reconnaissent comme valides les fausses clefs utilisées.

[1] Quelqu'un, entre le logiciel de consultation et le service de communication au public en ligne, écoute la conversation, alors que cette conversation est supposée être chiffrée de bout en bout, c'est un *man in the middle*.

Cette technique de blocage est donc l'une des plus coûteuses qu'on puisse imaginer, demandant des coopérations larges, et entraîne une analyse systématique des contenus des échanges avec le site, qu'ils portent sur la partie bloquée ou non.

Blocage par domaine et protocole Ce blocage suppose également une interception, qui peut se réaliser facilement si elle porte sur tout un domaine, en injectant dans le service de DNS de l'opérateur une fausse information sur l'adresse associée au nom de domaine. Le trafic ainsi redirigé est ensuite filtré : tout ce qui concerne les protocoles à bloquer est bloqué, tout le reste est renvoyé au service de manière transparente.

Cette technique est relativement peu coûteuse, en ce qu'elle ne demande pas d'intervention majeure sur le cœur du réseau des opérateurs.

Blocage par nom de domaine Ce blocage est le plus simple à réaliser. Il est, de fait, mis en œuvre par les personnes fournissant un service de DNS[2]. En pratique, le blocage se fait en ajoutant dans le DNS de l'opérateur un faux enregistrement associé au nom de domaine bloqué, qui le masque et est renvoyé à la place de la vraie réponse.

Le blocage porte en pratique sur un nom de domaine et sur toutes ses ramifications. Ainsi, si le domaine `monsite.fr` est bloqué, le service fourni directement par `monsite.fr` est bloqué, ainsi que celui fourni par `exemple.monsite.fr`. Une erreur dans le choix, visant le nom d'une plateforme d'hébergement plutôt que le nom d'un service hébergé, peut entrainer un surblocage massif.

Cette technique est de loin la moins coûteuse puisqu'elle n'entraîne qu'un coût technique marginal, ne restant que le coût des procédures de mise en place et de suivi des échanges sécurisés avec l'administration.

Il résulte de ce qui précède que la confusion terminologique du décret renvoie à trois techniques différentes de blocage ayant des conséquences techniques et pécuniaires fort différentes.

[2]L'usage commercial est que les abonnés à Internet utilisent le service de DNS gracieusement mis à leur disposition par leur fournisseur d'accès à Internet. Mais la fourniture de services DNS existe, en général à titre gracieux dans le cadre d'une autre offre, chez un grand nombre de prestataires de services de la société de l'information.

2. DISCUSSION — Intérêt à agir

2.1. French Data Network

FDN est une association loi 1901, et est un fournisseur d'accès à Internet. Elle existe, et exerce son activité depuis 1992, ce qui en fait le plus ancien fournisseur d'accès français à Internet encore en activité. Elle regroupe 450 adhérents et est administrée de manière entièrement bénévole. Elle ne fournit d'accès à Internet qu'à ses membres. Son intérêt à agir, en l'espèce est donc double.

D'une part, en tant qu'opérateur d'un réseau de communication ouvert au public, déclaré auprès de l'ARCEP, le décret attaqué lui est applicable directement. À ce titre, FDN fournit également un certain nombre de services (courrier électronique, hébergement de sites web ou de serveurs, etc) à ceux de ses membres qui en ont fait le choix.

D'autre part, en tant qu'association, représentant ses membres, y compris ceux auxquels elle fournit un accès à Internet, ses abonnés sont concernés au premier chef par les mesures restrictives de liberté mises en œuvre par le décret attaqué.

L'intérêt à agir de FDN a été reconnu par le Conseil d'État dans l'affaire n° 342405, par exemple.

2.2. La Quadrature du Net

La Quadrature du Net est une association loi 1901. Son objet général est la défense des droits fondamentaux dans l'environnement numérique. À ce titre, elle intervient dans les débats réglementaires touchant au droit de l'Internet aux niveaux français et européen, notamment en développant des analyses juridiques, en proposant et en évaluant des amendements au cours des procédures législatives.

Dès 2008 et 2009, LQDN s'était illustrée comme l'un « des fers de lance de l'opposition à la loi » HADOPI, selon l'expression du journal Le Figaro[1]. Elle avait à cette occasion porté de nombreux arguments juridiques plus tard validés dans la décision n° 2009-580 DC du Conseil constitutionnel du 10 juin 2009. Son combat contre les excès du droit d'auteur l'a également conduite à mener campagne contre le projet d'accord multilatéral ACTA,

[1] `https://www.laquadrature.net/fr/le-figaro-bataille-politique-autour-de-la-loi-antipiratage`

rejeté par le Parlement européen à l'été 2012.

L'un des axes forts de ses positions est la défense d'une protection judiciaire des droits fondamentaux sur Internet, et notamment la liberté d'expression et de communication. À ce titre, elle s'oppose à la délégation de la répression des infractions aux acteurs privés ou administratifs. En 2009, elle avait dans ce but proposé et défendu l'amendement dit « 138 » lors de l'examen du Paquet Télécom au Parlement européen. Ces derniers mois, elle s'est également illustrée dans les débats parlementaires français sur différents projets et propositions de loi tendant à étendre les obligations des hébergeurs en matière de surveillance des contenus, pointant le risque de censure extrajudiciaire qu'emportaient de telles mesures.

Cette défense de l'État de droit l'a évidemment conduite à se mobiliser sur les questions de vie privée et de surveillance des communications sur Internet. Au niveau européen, elle mène par exemple campagne sur le projet de règlement relatif à la protection des données personnelles. Au niveau français, LQDN s'est notamment illustrée par son opposition à la loi de programmation militaire (LPM) adoptée fin 2013. Elle participe depuis à l'Observatoire des Libertés Numériques, créé suite à la mobilisation de la société civile contre l'article 20 de la LPM, aux côtés entre autres de la Ligue des Droits de l'Homme et du Syndicat de la Magistrature. Récemment, elle a encore été auditionnée par le Conseil d'État le 28 janvier 2014 en vue de l'élaboration de son étude annuelle pour l'année 2014 intitulée « Le numérique et les droits fondamentaux ».

Enfin, les statuts de l'association lui confèrent la possibilité d'ester en justice – possibilité qu'elle entend exercer à l'occasion de ce recours.

Par le passé, La Quadrature du Net a déjà eu l'occasion d'intervenir auprès de juridictions. En 2011, elle était intervenue auprès du Conseil constitutionnel au travers d'un mémoire en « amicus curiae » pour pointer le caractère disproportionné et dès lors inconstitutionnel des mesures de blocage administratif de sites inscrit à l'article 4 de la loi LOPPSI[2]. Actuellement, elle participe à une tierce intervention d'une coalition d'ONG européennes auprès de la Cour européenne des droits de l'Homme, à l'occasion du recours de plusieurs associations britanniques contre le programme de surveillance d'Internet TEMPORA, révélé par Edward Snowden[3].

Plus récemment elle a introduit un recours pour excès de pouvoir devant le Conseil d'État contre le décret n° 2014-1576 du 24 décembre 2014 relatif à l'accès administratif aux données de connexion publié au Journal officiel de la République française n° 298 du 26 décembre 2014, p. 22224.

À de très nombreuses reprises, La Quadrature du net s'est opposée à l'introduction de mesures de blocages de sites Internet. Comme il sera exposé, ces mesures emportent une atteinte disproportionnée à la liberté d'expression ainsi qu'à d'autres droits et libertés que La Quadrature du Net a pour objet statutaire de défendre.

Ainsi, La Quadrature du Net introduit la présente requête non seulement en conformité avec ses statuts, mais aussi en pleine cohérence avec ses activités.

Par ailleurs, La Quadrature du Net agit en tant que représentant de l'ensemble de

[2] http://www.laquadrature.net/files/20110214_La\%20Quadrature\%20du\%20Net_Amicus\%20curiae\%20LOPPSI2.pdf

[3] https://www.laquadrature.net/fr/la-quadrature-sengage-dans-la-lutte-juridictionnelle-contre-la-surveillance-de-masse

ses membres, concernés par la conservation des données de connexion, l'intrusion qu'elle représente dans leur vie privée, et les accès de l'administration à ces données.

2.3. Fédération des fournisseurs d'accès à Internet associatifs

La Fédération FDN regroupe 28 fournisseurs d'accès à Internet associatifs, dont 27 sont des associations de droit français (loi de 1901 ou droit spécifique d'Alsace Moselle, selon le cas), la 28^{e} étant une association de droit belge. Toutes ces associations sont gérées de manière bénévole et représentent, toutes ensemble, près de 2000 adhérents. FDN est une des associations membres, et fondatrice, de la Fédération FDN. Les associations membres de la Fédération FDN sont toutes signataires d'une charte par laquelle elles prennent des engagements éthiques et techniques.

Ici encore, l'intérêt à agir de la Fédération FDN est double.

D'une part, en tant que représentant de 28 opérateurs, tous déclarés auprès du régulateur national, et presque tous de droit français, donc tous concernés par le décret attaqué qui leur est applicable.

D'autre part, en tant que représentant, au travers de ses membres, de l'ensemble des abonnés et adhérents de ses associations membres, concernés par les mesures restrictives de libertés mises en œuvre par le décret attaqué.

Par la présente requête conjointe, ces trois associations demandent l'annulation du décret attaqué, en ce qu'il est illégal tant en la forme que sur le fond.

3. DISCUSSION — Légalité externe

La décision attaquée est entachée de vices d'incompétence et de procédure.

3.1. Incompétences

3.1.1. Le décret attaqué porte une atteinte à la liberté de communication non prévue par la loi

L'article 6-1 de la LCEN impose aux opérateurs d'empêcher l'accès à certains services de communication au public en ligne. Le décret attaqué ajoute à cela l'obligation de rediriger le trafic vers une page d'information du ministère de l'intérieur.

En redirigeant vers une page du ministère de l'intérieur les personnes tentant d'accéder aux services dont l'accès est empêché, des données à caractère personnel identifiant de manière non-ambiguë l'internaute sont transmises au serveur du ministère de l'intérieur. De fait, le décret attaqué instaure une mesure de surveillance constitutive d'une restriction de la liberté de communication des pensées et des opinions. Ce faisant, le pouvoir réglementaire a outrepassé le champ des compétences qui lui sont dévolues par la Constitution.

En droit,

L'article 34 de la Constitution dispose que :

> *« La loi fixe les règles concernant :*
> *« - les droits civiques et les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques ; la liberté, le pluralisme et l'indépendance des médias ; les sujétions imposées par la défense nationale aux citoyens en leur personne et en leurs biens ; »*

Aux termes de l'article 11 de la Déclaration de 1789 :

> *« La libre communication des pensées et des opinions est un des droits les plus précieux de l'homme : tout citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la loi. »*

Le Conseil constitutionnel a précisé, dans sa décision n° 2009-577 DC du 3 mars 2009, que :

> *« La libre communication des pensées et des opinions, garantie par l'article 11 de la Déclaration de 1789 ne serait pas effective si le public auquel s'adressent les moyens de communication audiovisuels n'était pas à même de disposer, aussi bien dans le cadre du secteur privé que dans celui du secteur public, de programmes qui garantissent l'expression de tendances de caractère différent en respectant l'impératif d'honnêteté de l'information. En définitive,* ***l'objectif à réaliser est que les auditeurs et les téléspectateurs, qui sont au nombre des destinataires essentiels de la liberté proclamée par l'article 11, soient à même d'exercer leur libre choix sans que ni les intérêts privés ni les pouvoirs publics puissent y substituer leurs propres décisions.*** *»*

Ainsi, le législateur dispose d'un monopole pour limiter l'exercice des droits et libertés reconnus par la Constitution, notamment la liberté de communication.

Par ailleurs, la Cour européenne des droits de l'homme (Cour EDH) considère qu'une *simple menace de surveillance* constitue en soi une atteinte à la liberté de communication :

> *« [...] la législation elle-même 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 et constituant par là une « ingérence d'une autorité publique » dans l'exercice du droit des requérants au respect de leur vie privée et familiale ainsi que de leur correspondance. »*
> *(Arrêt Klass et autres contre Allemagne, Cour EDH, Plén., 6 septembre 1978, n° 5029/71, § 41)*

Ainsi, au regard de ces règles, seule la loi peut autoriser une mesure créant une menace de surveillance contraire à l'exercice de la liberté de communication.

En l'espèce,

L'article 3, alinéa 4, du décret attaqué dispose que :

> *« Les utilisateurs des services de communication au public en ligne auxquels l'accès est empêché sont dirigés vers une page d'information du ministère de l'intérieur, indiquant pour chacun des deux cas de blocage les motifs de la mesure de protection et les voies de recours. »*

Cette disposition, qui n'est pas prévue par la loi, oblige les fournisseurs d'accès à Internet à rediriger les connexions tentant d'atteindre un service dont l'accès est empêché vers une page d'information du ministère de l'intérieur.

Lors de cette opération, de nombreuses données à caractère personnel concernant les personnes à l'origine de ces connexions sont automatiquement transmises au service du ministère de l'intérieur hébergeant cette page d'information. Ce transfert est un impératif technique dicté par la mesure même. Au nombre des données transmises figurent au moins l'adresse IP, des cookies (fichiers d'identification stockés sur le logiciel de consultation et

envoyés automatiquement vers le logiciel serveur) et des informations sur les logiciels et terminaux utilisés. Ensemble, ces données permettent indéniablement l'identification, directement ou indirectement, des personnes concernées.

Ce faisant, tout citoyen a conscience que, lorsqu'il recherche des informations sur Internet, pèse le risque que le ministère de l'intérieur soit directement informé de sa tentative d'accéder à certaines informations et de son identité.

Il en résulte un sentiment de surveillance exercé par le pouvoir exécutif sur les sites — licites ou non — que les personnes consultent, modifiant leur comportement de recherche et d'accès à l'information sur Internet, ce qui constitue indéniablement une limite à l'exercice de leur liberté de communication.

En conclusion,

Les atteintes à la liberté de communication portées par l'article 3, alinéa 4 du décret attaqué n'étant pas prévues par le législateur, le pouvoir réglementaire n'est pas compétent pour les édicter.

Ainsi, l'article 3, alinéa 4, du présent décret viole l'article 34 de la Constitution ainsi que les articles 4 et 11 de la Déclaration des droits de l'homme et du citoyen en restreignant la liberté de communication des pensées et des opinions. C'est pourquoi il doit être annulé.

3.1.2. Le décret porte une atteinte au secret des correspondances non prévue par la loi

En droit,

L'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (Convention EDH) dispose que :

> *« 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.*
>
> *« 2.* ***Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi*** *et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. »*

De même, le Conseil constitutionnel considère :

> *« qu'il incombe au législateur d'assurer la conciliation entre, d'une part, la prévention des atteintes à l'ordre public et la recherche des auteurs d'infractions, toutes deux nécessaires à la sauvegarde de droits et de principes de valeur constitutionnelle, et, d'autre part, l'exercice des libertés constitutionnellement garanties ; qu'au nombre de celles-ci figurent la liberté d'aller et venir, l'inviolabilité du domicile privé, le secret des correspondances et le respect de la vie privée, protégés par les articles 2 et 4 de la Déclaration de 1789 [...] »*

(Conseil constitutionnel, décision n° 2004-492 DC du 02 mars 2004)

Enfin, l'article L. 241-1 du code de la sécurité intérieure dispose que :

> *« Le secret des correspondances émises par la voie des communications électroniques est garanti par la loi. Il ne peut être porté atteinte à ce secret que par l'autorité publique, dans les seuls cas de nécessité d'intérêt public prévus par la loi et dans les limites fixées par celle-ci. »*

Il en résulte un monopole du législateur pour prévoir les cas d'atteinte au secret des correspondances.

En l'espèce,

L'article 2, alinéa 3, du décret attaqué dispose que :

> *« Les adresses électroniques figurant sur la liste comportent soit un nom de domaine (DNS), soit un nom d'hôte caractérisé par un nom de domaine précédé d'un nom de serveur. »*

Son article 3, alinéa 1 dispose que :

> *« [Les opérateurs] empêchent par tout moyen approprié l'accès aux services fournis par les adresses électroniques figurant sur la liste et le transfert vers ces services. »*

Son article 3, alinéa 4 dispose que :

> *« Les utilisateurs des services de communication au public en ligne auxquels l'accès est empêché sont dirigés vers une page d'information du ministère de l'intérieur, indiquant pour chacun des deux cas de blocage les motifs de la mesure de protection et les voies de recours. »*

Comme cela a été expliqué section 1.2.2 page 6, la notion d'« adresses électroniques » visée par le decret attaqué peut désigner des adresses URL, des noms de domaine sur le protocole Web ou de simples noms de domaine.

La récente mise en œuvre par l'administration des mesures prévues au présent décret a révélé que celle-ci interprète cette notion comme désignant de simples noms de domaines.

Cette interprétation a pour conséquence technique que les opérateurs, devant rediriger les connexions tentant d'atteindre les services bloqués vers la page d'information du ministère de l'intérieur, doivent modifier leurs serveurs DNS pour remplacer l'adresse IP associée au nom de domaine du service bloqué par l'adresse IP d'un serveur sous la responsabilité du ministère de l'intérieur.

Ainsi, toute communication émise à destination de ce nom de domaine est redirigée vers le service du ministère de l'intérieur hébergeant la page d'information, quel que soit le protocole de communication utilisé. Par exemple, si le service ayant pour nom de domaine `monsite.fr` était bloqué, un courrier électronique envoyé à l'adresse `martin@monsite.fr` serait automatiquement redirigé vers les services du ministère de l'intérieur, sans que ni l'émetteur ni le destinataire de ce courrier ne puissent systématiquement l'anticiper.

Ainsi, sont redirigées vers les services du ministère de l'intérieur les communications émises à destination des toutes les personnes utilisant pour leur correspondance électronique privée le nom de domaine d'un service bloqué.

En conclusion,

À interpréter la notion d'« adresses électroniques » comme désignant de simples noms de domaine, l'article 3, alinéa 4, porte atteinte au secret de la correspondance d'un nombre potentiellement considérable de personnes, sans que le législateur ne l'ait prévu.

Ainsi, en échouant à définir correctement la notion d'« adresses électroniques », l'article 3, alinéa 4, du présent décret viole l'article 34 de la Constitution, les articles 2 et 4 de la Déclaration de 1789, l'article 8 de la Convention EDH ainsi que l'article L. 241-1 du code de la sécurité intérieure. C'est pourquoi il doit être annulé.

3.2. Vices de procédure

3.2.1. Absence d'arrêté autorisant le traitement de données à caractère personnel par l'administration

L'article 26, I, de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés dispose que :

> *« Sont autorisés par arrêté du ou des ministres compétents, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés, les traitements de données à caractère personnel mis en œuvre pour le compte de l'Etat et :*
> *« 1° Qui intéressent la sûreté de l'Etat, la défense ou la sécurité publique ;*
> *« 2° Ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté.*
> *L'avis de la commission est publié avec l'arrêté autorisant le traitement. »*

Au sens de la loi du 6 janvier 1978 précitée :

> *« Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur [des données à caractère personnel], quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, **la communication par transmission, diffusion ou toute autre forme de mise à disposition**, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction. »*

Or, comme décrit section 3.1.1 page 13, les services du ministère de l'intérieur hébergeant la page d'information vers laquelle sont redirigés les internautes tentant d'accéder aux sites bloqués collectent de façon systématique des données à caractère personnel les concernant.

Le traitement qui résulte nécessairement de cette redirection constitue un traitement de données à caractère personnel. Ce traitement de données s'inscrit dans un cadre qui intéresse bien la sûreté de l'État, la défense ou la sécurité publique.

En revanche, aucun arrêté n'a expressément autorisé ce traitement de données, et par conséquent la Commission nationale de l'informatique et des libertés n'a pas pu rendre l'avis motivé qui devait précéder sa mise en œuvre.

En conclusion, le présent décret, au quatrième alinéa de son article 3, viole l'article 26, I, de la loi du 6 janvier 1978 précitée et devra, de ce chef, être annulé.

3.2.2. Absence d'étude d'impact antérieure au décret

D'après la circulaire du 17 février 2011 relative à la simplification des normes concernant les entreprises et les collectivités territoriales :

> *« L'élaboration de tout projet de loi, d'ordonnance, de décret ou d'arrêté comportant des mesures concernant les entreprises, c'est-à-dire susceptibles d'avoir une incidence sur elles, tout particulièrement sur les petites et moyennes entreprises et sur les entreprises du secteur industriel, appelle une analyse d'impact circonstanciée.*
>
> *« S'agissant des projets d'ordonnance, de décret et d'arrêté, cette évaluation préalable sera retracée dans la fiche d'impact de l'annexe III de la présente circulaire.*
>
> *« Le commissaire à la simplification* ***doit être saisi*** *du projet de texte et de l'analyse d'impact correspondante :*
>
> *[...]*
>
> *« — s'agissant des projets de décret en Conseil d'État ou d'ordonnance, au plus tard concomitamment à la saisine des instances obligatoirement consultées si le projet entre dans leur champ de compétence et préalablement à l'organisation d'une réunion interministérielle ou saisine du cabinet du Premier ministre pour arbitrage et, en toute hypothèse, à la saisine du Conseil d'État. »*

Cette circulaire, adoptée par le Premier ministre, crée une obligation pour l'ensemble des composantes du Gouvernement et de l'administration non seulement d'élaborer une fiche d'impact mais de saisir le commissaire à la simplification du projet de décret, à tout le moins lors de la saisine du Conseil d'État.

Cette obligation s'applique lorsque sont en cause des mesures concernant les entreprises et tout particulièrement des petites et moyennes entreprises. Ce qui est le cas, comme en témoigne l'existence même d'associations comme celles de la Fédération FDN parmi les plus de 1600 opérateurs déclarés auprès du régulateur.

Le décret attaqué, en ce qu'il comporte des mesures concernant les fournisseurs d'accès à Internet — dont un grand nombre sont des petites et moyennes entreprises, voire des associations — devait être précédé d'une étude d'impact ainsi que d'une saisine du commissaire à la simplification. Or, il n'en a rien été.

Ainsi, le décret a été adopté en contradiction des dispositions contraignantes précitées et devra donc être annulé.

4. DISCUSSION — Légalité interne

La décision attaquée doit au surplus être annulée en ce qu'elle est contraire au droit de l'Union européenne et à la Convention EDH, à la loi, aux principes généraux du droit ainsi qu'à la Constitution.

À titre liminaire, il doit d'ores et déjà être précisé que les associations requérantes formeront une question prioritaire de constitutionnalité dans un mémoire séparé qui sera communiqué ultérieurement.

4.1. Le décret viole la séparation des pouvoirs

Le décret attaqué confie à l'autorité administrative le soin de qualifier un service de délictueux au sens des articles 421-2-5 et 227-23 du code pénal et de prendre des mesures répressives à leur égard. En cela, le décret attaqué viole la Constitution et l'article 16 de la Déclaration des droits de l'homme et du citoyen.

En droit,

L'article 16 de la Déclaration des droits de l'Homme et du citoyen de 1789 dispose que :

> *« Toute Société dans laquelle la garantie des Droits n'est pas assurée, ni la séparation des Pouvoirs déterminée, n'a point de Constitution. »*

Comme le Conseil constitutionnel l'a jugé encore récemment :

> *« [L]'article 16 de la Déclaration de 1789 implique le respect du caractère spécifique des fonctions juridictionnelles, sur lesquelles ne peuvent empiéter ni le législateur ni le Gouvernement[...] »*
> *(Conseil constitutionnel, décision nº 2011-192 QPC du 10 novembre 2011, considérant 21)*

Dans sa décision nº 2005-532, le Conseil constitutionnel a précisé le principe de la séparation des pouvoirs en jugeant que :

« [Les] mesures de police purement administrative [...] ne sont pas placées sous la direction ou la surveillance de l'autorité judiciaire, mais relèvent de la seule responsabilité du pouvoir exécutif ; qu'elles ne peuvent donc avoir d'autre finalité que de préserver l'ordre public et de prévenir les infractions ; que, dès lors, en indiquant qu'elles visent non seulement à prévenir les actes de terrorisme, mais encore à les réprimer, le législateur a méconnu le principe de la séparation des pouvoirs ; »

(Conseil constitutionnel, nº 2005-532 DC du 19 janvier 2006, considérant 5)

Le principe de la séparation des pouvoirs implique donc que le pouvoir de réprimer un comportement relève exclusivement de l'autorité judiciaire, à l'exclusion du Gouvernement et du législateur. Par exception, ce pouvoir exclusif peut être partagé avec une autorité administrative indépendante disposant d'un « pouvoir de sanction dans la mesure nécessaire à l'accomplissement de sa mission » (Cons. const. décision nº 88-248 DC du 17 janvier 1989, considérant 27).

Le pouvoir de réprimer se composant de deux pouvoirs - celui de juger quels comportements doivent être réprimés et celui de juger par quelle peine la répression doit s'exercer - en matière pénale, l'autorité judiciaire a le pouvoir exclusif de juger qu'un comportement constitue un délit ou un crime et par quelle peine le sanctionner.

L'article 6-1 de la LCEN quant à lui dispose, en son deuxième alinéa, que :

*« [L]'autorité administrative peut notifier aux [fournisseurs d'accès à Internet] la liste des adresses électroniques des services de communication au public en ligne **contrevenant auxdits articles 421-2-5 et 227-23**. Ces personnes doivent alors empêcher sans délai l'accès à ces adresses. »*

Cette disposition confère à une autorité administrative le pouvoir d'exiger d'un fournisseur d'accès à Internet qu'il bloque l'accès aux services contrevenant aux articles 421-2-5 et 227-23 du code pénal précités, sans toutefois renvoyer à une décision de l'autorité judiciaire antérieure qualifiant ainsi ces services, conformément au principe de la séparation des pouvoirs.

En l'espèce,

L'article 4 du présent décret dispose :

« L'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication vérifie au moins chaque trimestre que le contenu du service de communication contrevenant présente toujours un caractère illicite.

« Lorsque ce service a disparu ou que son contenu ne présente plus de caractère illicite, l'office retire de la liste les adresses électroniques correspondantes [...] »

Cette disposition confie à l'OCLCTIC le pouvoir de lever le blocage d'un service s'il considère, selon ses propres vérifications, que ce service ne constitue plus l'un des délits prévus, sans donc qu'un juge n'ait eu à se prononcer sur la nature délictuelle de celui-ci.

L'article 2 du présent décret dispose :

> *« La liste des adresses électroniques des services de communication au public en ligne* ***contrevenant aux articles 227-23 et 421-2-5 du code pénal*** *est adressée aux personnes mentionnées au 1 du I de l'article 6 de la loi du 21 juin 2004 susvisée selon un mode de transmission sécurisé, qui en garantit la confidentialité et l'intégrité. »*

Cette disposition confie à l'OCLCTIC la mission de transmettre aux fournisseurs d'accès à Internet la liste des services constituant l'un des délits concernés, afin que l'accès en soit bloqué, sans toutefois exiger explicitement que seuls y figurent les services ainsi caractérisés par un juge.

Or, au vu de son article 4 précité, l'économie du présent décret indique que la mission confiée à l'OCLCTIC à son article 2 comprend aussi celle de définir seul la liste des services à bloquer, sans qu'un juge n'ait eut à décider s'ils constituaient l'un des délits concernés.

Le blocage opéré le 15 mars 2015 par l'OCLCTIC du site `http://www.islamic-news.info` confirme cette interprétation, aucun juge ne s'étant prononcé sur le caractère délictuel de ce service préalablement à son blocage.

Ainsi, comme le relève la Commission nationale consultative des droits de l'Homme au sujet des dispositions contestées :

> *« Le nouveau texte habilite l'autorité administrative à décider du blocage, alors même qu'une ou plusieurs infractions ont déjà été commises. Il ne peut donc être considéré qu'il s'agit d'une mesure de police purement administrative destinée à prévenir la provocation à des actes de terrorisme ou l'apologie de ceux-ci. Les nouvelles dispositions relèvent indéniablement du domaine de la police judiciaire dont la direction et le contrôle sont dévolus à l'autorité judiciaire, seule compétente pour la poursuite et la répression des infractions »*
>
> *(Avis sur le projet de loi renforçant les dispositions relatives à la lutte contre le terrorisme, adopté par l'Assemblée plénière de la CNCDH le 25 septembre 2014).*

De la sorte, par les article 2 et 4 du présent décret, l'administration s'est arrogée le pouvoir de qualifier un comportement de délit, alors que ce pouvoir relève de celui de réprimer, exclusif de l'autorité judiciaire selon le principe de la séparation des pouvoirs. L'OCLCTIC n'étant pas une autorité administrative indépendante, elle ne saurait bénéficier de l'exception pouvant lui laisser un pouvoir de sanction propre.

En conclusion,

En ce qu'ils confient à l'OCLCTIC le soin de qualifier seul un service comme contrevenant aux articles 421-2-5 et 227-23 du code pénal, les articles 2 et 4 du décret attaqué violent l'article 16 de la Déclaration des Droits de l'Homme et du Citoyen et l'article 6-1 de la LCEN et devront de ce chef être annulés.

4.2. Le décret n'est ni clair, ni intelligible

Le décret porte une atteinte disproportionnée aux principes de sécurité juridique et de confiance légitime ainsi qu'à l'objectif de valeur constitutionnelle de clarté et d'intelligibilité de la norme.

En droit,

Dans son arrêt *KPMG* du 24 mars 2006 (n° 288460, 288465, 288474, 288485), le Conseil d'État a jugé que le moyen selon lequel un acte administratif pouvait entraver l'objectif de valeur constitutionnelle de clarté et d'intelligibilité de la norme était opérant.

Dans le même arrêt, le Conseil d'État a jugé que :

> *« le principe de confiance légitime, qui fait partie des principes généraux du droit communautaire, ne trouve à s'appliquer dans l'ordre juridique national que dans le cas où la situation juridique dont a à connaître le juge administratif français est régie par le droit communautaire »*

L'article 1er de la directive 2002/58/CE 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 dispose que :

> *« La présente directive harmonise les dispositions des États membres nécessaires pour assurer un niveau équivalent de protection des droits et libertés fondamentaux, et en particulier du droit à la vie privée, en ce qui concerne le traitement des données à caractère personnel dans le secteur des communications électroniques, ainsi que la libre circulation de ces données et des équipements et des services de communications électroniques dans la Communauté. »*

En l'espèce,

Le décret met en œuvre un traitement de données à caractère personnel dans le secteur des communications électroniques qui affecte le niveau de protection des droits et libertés fondamentaux (voir section 3.1 page 12). Le principe de confiance légitime est donc bien invocable.

Quant au principe de sécurité juridique, son applicabilité est ici avérée en ce qu'il est un principe général du droit auquel les actes administratifs sont tous soumis. Et quant à l'objectif de clarté et d'intelligibilité, l'administration y est soumise au même titre que le législateur.

Or, le décret n'est ni clair, ni intelligible et porte ainsi atteinte à ces trois principes en ses articles 2 et 3.

L'article 2 du décret attaqué dispose que :

> *« Les adresses électroniques figurant sur la liste comportent soit un nom de domaine (DNS), soit un nom d'hôte caractérisé par un nom de domaine précédé d'un nom de serveur. »*

Et l'article 3 du décret attaqué dispose que :

> *« Dans un délai de vingt-quatre heures suivant la notification prévue au deuxième alinéa de l'article 6-1 de la loi du 21 juin 2004 susvisée, les personnes mentionnées au 1 du I de l'article 6 de la même loi empêchent par tout moyen approprié l'accès aux services fournis par les adresses électroniques figurant sur la liste et le transfert vers ces services. »*

Premièrement, cette disposition du décret relève du non-sens technique. Comme expliqué section 1.2.1 page 5,

- d'une part, un nom de domaine n'est pas un DNS ; un DNS désignant un annuaire faisant l'équivalence entre un nom de domaine et une adresse IP ;
  par conséquent, l'expression « un nom de domaine (DNS) » n'a aucun sens ;
- d'autre part, un nom d'hôte « caractérisé par un nom de domaine précédé d'un nom de serveur » n'est pas une notion techniquement et juridiquement intelligible ;
  la notion de « nom de serveur » ne renvoyant à aucune notion connue, y compris pour des spécialistes des réseaux Internet.

Deuxièmement, la notion d'« adresse électronique » n'est pas précisément définie par le décret attaqué. Comme expliqué section 1.2.2 page 6, cette notion, telle que présentée dans le décret attaqué, peut recouvrir trois situations :

1. L'adresse d'une page Web précise, alors appelée « adresse URL » (pour « Uniform resource locator »), pouvant ainsi se présenter : `http://monsite.fr/fichier.html`.
2. Un nom de domaine sur un protocole précis, pouvant ainsi se présenter, quant au protocole Web : `http://monsite.fr`.
3. Un nom de domaine, pouvant ainsi se présenter : `monsite.fr`.

Or, le sens plural que peut revêtir cette notion inédite en droit n'est pas sans conséquence. En effet, selon la forme technique que revêtira une « adresse électronique » telle que notifiée par l'autorité administrative en conformité avec le décret attaqué, alors les moyens de mise en œuvre de la mesure de blocage dont disposeront les fournisseurs d'accès à Internet sont loin d'être comparables. D'une part, leur mise en œuvre nécessiterait des interventions techniques plus ou moins lourdes et coûteuses et d'autre part l'impact de cette mise en œuvre sur les communications électroniques de leurs utilisateurs varie grandement.

1. S'il s'agit de bloquer l'accès à l'adresse URL d'une page Web précise, les opérateurs devraient surveiller l'ensemble des communications susceptibles de correspondre à cette adresse, analyser chacune d'elles et bloquer celles correspondant à l'adresse exacte, ce qui impliquerait de surveiller et d'analyser la totalité du trafic Internet, portant une atteinte significative au respect de la vie privée de l'ensemble des utilisateurs du réseau.
2. S'il s'agit de bloquer l'accès à un nom de domaine sur le protocole Web, les opérateurs devraient bloquer les requêtes de type `http://` vers le nom de domaine `monsite.fr`, auquel cas tous les services rattachés à ce nom de domaine seraient bloqués dans leur ensemble (par exemple, pour le site de YouTube, toutes les chaînes YouTube), portant une atteinte significative à la liberté de communication des utilisateurs d'accéder à des contenus licites.

3. S'il s'agit de bloquer globalement l'accès à un nom de domaine, les opérateurs devraient bloquer, non seulement, tous les services rattachés à ce nom de domaine mais, aussi, beaucoup plus largement, toute « *communication électronique* » à destination du même nom de domaine, incluant les communications privées (par exemple, celles adressées à l'adresse `utilisateur@monsite.fr`) qui seraient de surcroît redirigées vers le service du ministère de l'intérieur, comme expliqué section 3.1.2 page 14, portant ainsi, de plus, atteinte au secret des correspondances.

Enfin, il faut souligner qu'une formulation précise et rigoureuse de la notion d'« adresse électronique » était possible, par exemple en prenant des références techniques précises et sans ambiguïtés : « Les adresses électroniques figurant sur la liste sont des noms de domaines, assorties des noms des protocoles à destination de ces adresses qui doivent être bloqués ».

En conclusion,

En échouant à définir de façon cohérente ou univoque les notions qu'ils mobilisent et en exposant les fournisseurs d'accès aux peines prévues au 1 du VI de l'article 6 de la LCEN, les articles 2 et 3 du décret attaqué doivent être annulés en ce qu'ils portent une atteinte disproportionnée aux principes de sécurité juridique et de confiance légitime ainsi qu'à l'objectif de valeur constitutionnelle de clarté et d'intelligibilité de la norme.

4.3. Le blocage de sites porte une atteinte disproportionnée à la liberté d'expression

Tant la CJUE que la Cour EDH ont, au fil de leur jurisprudence, distingué plusieurs critères leur permettant d'évaluer la proportionnalité d'une restriction du droit à la liberté d'expression protégé par l'article 10 de la Convention EDH. Pour s'assurer de la proportionnalité d'une telle ingérence, les juridictions sont notamment conduites à examiner si elle est « *nécessaire dans une société démocratique* ». Cette expression signifie notamment que les mesures prescrites doivent effectivement atteindre l'objectif qu'on leur assigne, qu'elles ne doivent pas aller au-delà de ce qui est nécessaire pour atteindre l'objectif poursuivi, et que ces mêmes objectifs ne peuvent pas être satisfaits par des mesures moins restrictives de liberté.

Sur chacun de ces trois points, les mesures de blocage procédant de l'article 6-1 de la LCEN que le décret vient préciser sont entachées d'inconventionnalité.

4.3.1. Les mesures de blocage de sites sont inefficaces

Le décret attaqué instaure des mesures qui portent une atteinte disproportionnée à la liberté d'expression du fait de leur inefficacité. Cette dernière est en outre renforcée par les modalités techniques de blocage retenues par le gouvernement.

En droit,

Dans son arrêt *Telekabel*, la CJUE a estimé que pour être conforme au droit de l'Union, une mesure de blocage efficace doit avoir :

> *« pour effet **d'empêcher** ou, au moins, de **rendre difficilement réalisables** les consultations non autorisées des objets protégés et de **décourager sérieusement** les utilisateurs d'Internet ayant recours aux services du destinataire de cette même injonction de consulter les contenus illicites justifiant l'injonction judiciaire de blocage »*
> *(Arrêt UPC Telekabel c. Constantin Film Verleih et Wega, CJUE, affaire C-314/12, 27 mars 2014, § 64)*

En l'espèce,

L'article 6-1 de la LCEN dispose que :

> *« Lorsque les nécessités de la lutte contre la provocation à des actes terroristes ou l'apologie de tels actes relevant de l'article 421-2-5 du code pénal ou contre la diffusion des images ou des représentations de mineurs relevant de l'article 227-23 du même code le justifient, l'autorité administrative peut demander à toute personne mentionnée au III de l'article 6 de la présente loi ou aux personnes mentionnées au 2 du I du même article 6 de retirer les contenus qui contreviennent à ces mêmes articles 421-2-5 et 227-23. Elle en informe simultanément les personnes mentionnées au 1 du I de l'article 6 de la présente loi. En l'absence de retrait de ces contenus dans un délai de vingt-quatre heures, l'autorité administrative peut notifier aux personnes mentionnées au même 1 la liste des adresses électroniques des services de communication au public en ligne contrevenant auxdits articles 421-2-5 et 227-23. »*

Dans l'étude d'impact de la LOPPSI, le Gouvernement résumait les deux objectifs assignés aux mesures administratives de blocage : d'une part à « prévenir l'accès involontaire des internautes » s'y trouvant confrontés par inadvertance et, d'autre part, « complexifier l'accès volontaire » par des personnes cherchant activement à accéder à ces contenus.

Le 15 mars 2015, le site `islamic-news.info` était bloqué. La page d'information du ministère de l'intérieur indique que cette mesure de blocage est prise :

- *Pour protéger les internautes, afin qu'ils ne se trouvent pas confrontés à des contenus violents et contraires à la loi.*
- *Pour que les personnes qui tentent de visionner ces contenus puissent prendre conscience de la gravité de tels actes.*
- *Pour lutter contre les sites qui font l'apologie ou qui provoquent directement à la commission d'actes de terrorisme.*

Pour chacun de ces objectifs, les mesures s'avèrent inadaptées et inefficaces.

L'étude d'impact réalisée par le gouvernement en amont de l'adoption de la LOPPSI prévoyait « *de renvoyer à un décret d'application la fixation des modalités d'application de ce dispositif, notamment la définition des dispositifs techniques utilisés* ».

Si les textes d'application demeurent en fait silencieux sur la nature technique des mesures de blocage, de nombreuses interventions publiques émanant tant de l'administration que des opérateurs ont depuis permis de confirmer informellement le choix du ministre de l'intérieur d'avoir recours à la technique de blocage par nom de domaine.

Or, en dépit des dires du ministre, cette méthode n'est pas respectueuse des libertés, et n'est guère efficace. En effet, le principal intérêt du blocage par nom de domaine réside en réalité dans sa facilité de mise en œuvre et son coût relativement peu élevé en comparaison à d'autres modalités de blocage. Mais le blocage par nom de domaine est également l'un des plus faciles à contourner.

De nombreux outils liés à l'utilisation d'Internet conduiront tant les utilisateurs de bonne que de mauvaise foi à contourner ces mesures destinées à les protéger, ne serait-ce que pour vouloir s'informer en connaissance de cause.

Parmi les mesures de contournement pouvant être adoptées figurent :

1. Le fait de s'abonner chez un fournisseur d'accès à Internet qui n'a pas été destinataire des demandes de blocage émanant de l'administration.
   À titre d'exemple, la demande de blocage du site `islamic-news.info` n'a pas été adressée aux requérants concernés (l'association French Data Network et les membres de la Fédération des fournisseurs d'accès à Internet associatifs).
2. Le fait d'utiliser un autre serveur DNS que celui proposé par leur fournisseur d'accès via les réglages de son navigateur Web. Une opération très simple à réaliser, et qui est notamment employée pour contourner le blocage (judiciaire) de sites diffusant sans autorisation des œuvres soumises au droit d'auteur.
3. Le fait d'utiliser des Virtual Private Networks (VPN), permettant d'accéder à Internet par un serveur situé dans une autre juridiction que celle où le blocage a été mis en place.
4. Le fait d'utiliser un outil de protection de la confidentialité des communications tel que le réseau Tor, qui permet selon un récent rapport de l'assemblée parlementaire du Conseil de l'Europe de protéger sa vie privée sur Internet[1].

Ensuite, s'agissant des éditeurs ou des hébergeurs des sites visés, il est également extrêmement aisé pour eux de s'affranchir des mesures de blocage prononcées à leur encontre. Par exemple, en migrant vers un autre nom de domaine, la mesure de blocage est rendue inefficace au regard des objectifs visés par le Gouvernement.

Au contraire, les mesures de blocage risquent de rendre la prévention et la répression des infractions qui motivent ces mesures encore plus difficiles, comme le relève le Conseil national du numérique dans son avis sur la loi du 13 novembre 2014 :

> *« Le dispositif proposé présente le risque de pousser les réseaux terroristes à complexifier leurs techniques de clandestinité, en multipliant les couches de cryptage et en s'orientant vers des espaces moins visibles du réseau, renforçant la difficulté du travail des enquêteurs. Certaines de ces techniques sont très faciles à utiliser et sont déjà maîtrisées par les tranches d'âge cibles des recruteurs, qui sont familiers de l'usage des Réseaux Privés Virtuels (VPN), du Peer-to-Peer (P2P) ou de TOR »*

[1] Omtzigt, Pieter, 26 janvier 2015. *Mass Surveillance*. Strasbourg, Assemblée parlementaire du Conseil de l'Europe, p. 13.

(avis n° 2014-3 du 15 juillet 2014 sur l'article 9 du projet de loi renforçant les dispositions relatives à la lutte contre le terrorisme).

Ces observations sont d'ailleurs confirmées par les déclarations du directeur général de l'Agence nationale de sécurité des systèmes d'information. Il indiquait avoir signalé « le problème de l'efficacité de ces mesures », expliquant être pour cette raison notamment « très réservé sur ces mesures d'un point de vue technique ».[2]

Pour ces raisons, le décret et la loi dont il procède ne répondent pas à l'exigence conventionnelle d'efficacité de la mesure. Pour bloquer les sites visés, l'administration devrait recourir à d'autres modalités techniques que celles annoncées par le Gouvernement, mais qui seraient à la fois plus coûteuses et qui constitueraient une ingérence disproportionnée dans le droit à la vie privée.

En effet, comme le remarque le Conseil national du numérique dans son avis précité :

« Pour être efficace, un dispositif de blocage devrait être capable d'analyser finement le contenu même de ces échanges personnels. Ces techniques d'inspection profonde relèveraient non seulement de la censure, mais aussi de l'atteinte à la vie privée et à la liberté de conscience, et seraient inadmissibles en tant que telles ».

De fait, les dispositions attaquées risquent d'encourager l'adoption de techniques de contournement par certaines personnes souhaitant accéder à ces contenus et légitimer l'adoption ultérieure de mesures encore plus restrictives de liberté — un phénomène d'ailleurs caractéristique de l'évolution du droit encadrant la liberté de communication sur Internet où les mesures inefficaces encouragent des comportements sociaux d'évitement du droit qui eux-mêmes suscitent de nouvelles mesures répressives. Cette fuite porte un grave préjudice au triple objectif de protection des droits fondamentaux, d'efficacité et de qualité de la loi.

En conclusion,

Compte tenu de la facilité avec laquelle le blocage par nom de domaine peut être contourné, à la fois par des internautes de bonne foi et a fortiori par des personnes cherchant activement à accéder aux contenus visés, il ne peut être sérieusement défendu que ces mesures auront pour effet, comme l'impose la jurisprudence *Telekabel* de la CJUE, « d'empêcher » ou, au moins, « de rendre difficilement réalisables » ou de « décourager sérieusement » l'accès aux sites visés.

Ainsi, les mesures visées ne parviennent pas à atteindre les objectifs visés par le Gouvernement et sont dès lors disproportionnées.

[2] Rees, Marc, 2014. "L'ANSSI « très réservée » sur les mesures de blocage de sites." *Next Inpact*. 10 septembre 2014. Disponible à l'adresse : `http://www.nextinpact.com/news/89802-l-anssi-tres-reservee-sur-mesures-blocage-sites.htm`.

4.3.2. Les mesures de blocage impliquent d'importants effets collatéraux

Les dispositions de la décision attaquée régissant le blocage des sites visés apparaissent non-nécessaires et dès lors disproportionnées en raison du risque de blocage de contenus parfaitement licites, y compris de sites licites et distincts de ceux indiqués dans la liste transmise aux fournisseurs d'accès à Internet.

4.3.2.1. Effets collatéraux du blocage de noms de domaines

En droit,

Dans son arrêt *Yildrim* du 18 décembre 2012, la Cour EDH souligne l'absence de proportionnalité des mesures de blocage validées par les juridictions turques qui avaient pour effet de bloquer l'intégralité des sites hébergés par « Google Sites » en vue de bloquer un seul de ces sites. Les juges européens notent ainsi que :

> *« Dans leur décision, les juges ont retenu uniquement que le seul moyen de bloquer l'accès au site litigieux conformément à la décision rendue en ce sens était de bloquer totalement l'accès à Google Sites. Or, de l'avis de la Cour, ils auraient dû notamment* ***tenir compte du fait que pareilles mesures rendant inaccessibles une grande quantité d'informations affectent considérablement les droits des internautes et ont un effet collatéral important*** *» (§ 66).*

La Cour EDH note dans le même arrêt que :

> *« (. . .)* ***la mesure en cause a eu des effets arbitraires et ne saurait être considérée comme visant uniquement à bloquer l'accès au site litigieux*** *car elle consistait en un blocage général de tous les sites hébergés par Google Sites. En outre, le contrôle juridictionnel du blocage de l'accès aux sites Internet ne réunit pas les conditions suffisantes pour éviter les abus :* ***le droit interne ne prévoit aucune garantie pour éviter qu'une mesure de blocage visant un site précis ne soit utilisée comme moyen de blocage général*** *» (§ 68).*

Dans son arrêt *Akdeniz c. Turquie* du 11 mars 2014, la Cour EDH confirme cette jurisprudence :

> *« (. . .) une mesure de blocage de l'accès à un site web devait s'inscrire dans un cadre légal particulièrement strict quant à la délimitation de l'interdiction et efficace quant au contrôle juridictionnel contre les éventuels abus, car* ***elle pouvait avoir des effets de « censure collatérale » importants*** *» (§28).*

Dans son arrêt du 27 mars 2014 *UPC Telekabel* précité, la CJUE a estimé que pour être conforme au droit de l'Union, et en particulier à l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'UE, une mesure de blocage devait respecter la condition selon laquelle :

> *« (. . .)* ***les mesures prises ne privent pas inutilement*** *les utilisateurs d'Internet de la possibilité d'accéder de façon licite aux informations disponibles » (§63).*

Au paragraphe 56 de l'arrêt, la CJUE souligne en outre que :

> *« (. . .) les mesures qui sont adoptées par le fournisseur d'accès à Internet doivent être* ***strictement ciblées****, en ce sens qu'elles doivent servir à mettre fin à l'atteinte portée par un tiers au droit d'auteur ou à un droit voisin,* ***sans que les utilisateurs d'Internet ayant recours aux services de ce fournisseur afin d'accéder de façon licite à des informations s'en trouvent affectés****. À défaut, l'ingérence dudit fournisseur dans la liberté d'information desdits utilisateurs s'avérerait injustifiée au regard de l'objectif poursuivi » (§56).*

En l'espèce,

En dépit du manque de clarté de la nature des mesures de blocages que les fournisseurs d'accès à Internet devront mettre en œuvre, le mode de blocage retenu jusqu'à présent par le ministère de l'intérieur consiste à demander le blocage d'une liste de noms de domaines.

Or, non seulement le blocage par nom de domaine n'apporte aucune garantie permettant de s'assurer que la mesure d'interdiction sera limitée aux contenus justifiant l'interdiction, comme l'exige la jurisprudence, mais il comporte au contraire des risques particulièrement élevés de blocage collatéral.

Dans son étude d'impact sur la LOPPSI, le Gouvernement reconnaît d'ailleurs lui-même que :

> *« ce système comporte plusieurs inconvénients : l'ensemble des services proposés sur le domaine concerné sont bloqués : les pages Web mais aussi les méls, le tchat... Ce système comporte intrinsèquement un risque de "sur-blocage" »*

En effet, lorsqu'un nom de domaine est bloqué par un fournisseur d'accès, l'ensemble des contenus et services licites qu'il héberge le sont aussi.

La mesure de blocage, que le Gouvernement présente comme une mesure préventive, a donc pour effet de bloquer l'ensemble des contenus licites également présents sur le service de communication au public en ligne visé.

En outre, au-delà des contenus licites présents sur les sites visés, le blocage par nom de domaine risque de bloquer de nombreux autres services de communication au public en ligne hébergés sous le même nom de domaine, à l'image des effets collatéraux dénoncés par la Cour EDH dans l'arrêt *Yildrim* précité.

Ainsi, en 2011, la saisie de dix noms de domaine par la police américaine dans le cadre d'une opération contre la diffusion d'images pédopornographiques avait pour ces mêmes raisons conduit au blocage accidentel de 84 000 sites. Les internautes souhaitant accéder à ces sites parfaitement licites étaient dès lors confrontés à une page Web publiée par les autorités américaines expliquant les motif justifiant cette censure, faisant dès lors porter sur les gestionnaires de ces sites des accusations particulièrement graves et infamantes. Il en sera de même lorsque les mesures de blocage enjointes par l'administration française conduiront à des cas de surblocage, d'ailleurs extrêmement courants dans tous les pays qui les pratiquent à grande échelle, et ce même lorsqu'ils recourent à des techniques plus ciblées (voir le cas du Royaume-Uni par exemple, où les opérateurs recourent généralement au blocage dit « hybride » dans le cadre d'un régime d'« autorégulation »). Plusieurs cas de surblocage ont été recensés par l'association requérante La Quadrature du Net, à l'adresse suivante : `https://wiki.laquadrature.net/Surblocage`.

En conclusion,

Les risques de sur-blocage étant particulièrement élevés s'agissant de la technique de blocage par nom de domaine, les dispositions attaquées portent une atteinte disproportionnée aux libertés et sont dès lors en violation de la jurisprudence de la Cour EDH et de la CJUE.

Par ailleurs, comme expliqué section 1.2.1 page 5, les mesures de blocage peuvent avoir pour conséquence d'intercepter, non seulement, tout le trafic du « *service de communication au public en ligne* » mais, aussi, de manière collatérale, toute « *communication électronique* » à destination du même nom de domaine, incluant les communications privées ; par exemple, celles adressées à l'adresse `utilisateur@monsite.fr`, que ce soit par chat ou par courrier électronique.

Une telle mesure ne saurait s'analyser comme visant à assurer l'un des trois objectifs annoncés par le Gouvernement sur la page d'information susmentionnée. Elle constitue en revanche une grave atteinte au secret des correspondances, à la liberté d'expression ainsi qu'à la protection de la vie privée.

4.3.2.2. Effets collatéraux du blocage d'URL

En droit,

La Cour EDH considère qu'une *simple menace de surveillance* constitue en soi une atteinte à la liberté de communication :

> *« [...] la législation elle-même 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 et constituant par là une « ingérence d'une autorité publique » dans l'exercice du droit des requérants au respect de leur vie privée et familiale ainsi que de leur correspondance. »*
> *(Arrêt Klass et autres contre Allemagne, Cour EDH, Plén., 6 septembre 1978, § 41)*

D'autre part, la directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information dispose dans son article 15, l'absence d'obligation générale en matière de surveillance qui précise que :

> *« 1. Les États membres ne doivent pas imposer aux prestataires, pour la fourniture des services visée aux articles 12, 13 et 14, une obligation générale de surveiller les informations qu'ils transmettent ou stockent [...] »*

En l'espèce,

Comme indiqué section 1.2.2 page 6, les mesures de blocage peuvent concerner les adresses URL, en tant qu'« adresses électroniques », conformément aux caractéristiques données par le décret.

La mise en œuvre de cette mesure de blocage d'URL est laissée à l'appréciation du fournisseur d'accès à Internet, lequel peut procéder « par tout moyen approprié » (article 3 du décret attaqué).

Pour autant, la marge de manœuvre du fournisseur d'accès à Internet est restreinte par des nécessités techniques dont il ne peut s'affranchir, dues notamment au fonctionnement des réseaux Internet comme expliqué au point 1.2.3 page 7.

Les opérateurs sont alors soumis *ipso facto* à une **obligation générale de surveillance** de l'ensemble des communications afin d'intercepter celles susceptibles de correspondre à l'accès à une « adresse électronique » qui fait l'objet d'une mesure de blocage.

Par ailleurs, une partie importante des communications électroniques étant chiffrée (par exemple, si l'adresse visée comporte un protocole chiffré comme c'est le cas pour les sites de commerce en ligne, les sites bancaires, pour les sites manipulant des données personnelles et pour d'autres sites soucieux du respect de la vie privée des utilisateurs), la mesure de blocage implique que l'opérateur déchiffre ou intercepte les communications chiffrées entre un utilisateur et un service de communication au public en ligne, de manière à y distinguer celles relatives à une « adresse électronique » objet du blocage.

La mesure de blocage a donc des répercussions importantes sur le droit à la vie privée et la liberté de communication des utilisateurs de services de communication au public en ligne, puisque la mise en œuvre de ces mesures exacerberait le sentiment de surveillance ou la simple menace de surveillance dont souffriraient les utilisateurs de services de communication au public en ligne.

Cela a également pour conséquence de créer *de facto* une obligation générale de surveillance à la charge des opérateurs, en contradiction avec les engagements de la France au regard de la directive 2000/31/CE susvisée.

En conclusion,

C'est pourquoi la mesure de blocage d'URL emporte des effets collatéraux, lesquels ne sont aucunement nécessaires et dès lors, la mesure est disproportionnée au regard de ses objectifs légaux.

4.3.3. Il existe des mesures efficaces alternatives au blocage

La disproportion de l'atteinte portée par les dispositions attaquées à la liberté d'expression est enfin caractérisée par l'existence de mesures alternatives moins restrictives de droits.

En droit,

Lorsque la Cour EDH et la CJUE évaluent le caractère nécessaire d'une mesure portant atteinte à la liberté d'expression, elles cherchent à déterminer si des mesures alternatives moins restrictives des libertés fondamentales en jeu permettent de satisfaire l'objectif poursuivi. De ce point de vue, dans le but de prévenir ou de réprimer les abus à la

liberté d'expression, le retrait des contenus des serveurs constitue une mesure bien plus satisfaisante, et ce même si elle se heurte aux limites de la coopération internationale.

Ainsi, dans l'affaire *Yildrim c. Turquie*, la Cour EDH remarque, qu'à l'occasion du recours devant le tribunal d'instance pénal contre sa décision, l'autorité administrative turque en charge de la régulation des télécommunications (la PTI), qui avait initialement prononcé la mesures de blocage, avait indiqué aux juges « que c'était là la seule possibilité de bloquer le site litigieux, son propriétaire n'étant pas titulaire d'un certificat d'hébergement et se trouvant à l'étranger » (§10).

La Cour EDH observe à ce sujet que :

> *« (. . .) il convient d'observer que lorsque le tribunal d'instance pénal de Denizli a décidé de bloquer totalement l'accès à Google Sites en vertu de la loi n°5651,* ***il s'est contenté de se référer à un avis émanant de la PTI, et n'a pas recherché si une mesure moins lourde pouvait être adoptée pour bloquer l'accès au site litigieux*** *» (§64)*

Toute autorité publique ayant à juger de la légalité d'une mesure de blocage doit donc rechercher si une mesure moins restrictive de liberté peut être employée.

Enfin, le paragraphe 1 de l'article 10 de la Convention EDH précise que la sauvegarde de la liberté d'expression et des principes de la jurisprudence relative vaut « sans considération de frontière » (voir : CEDH, Association Ekin c. France, n° 39288/98, Association Ekin, § 62).

En l'espèce,

En premier lieu, la loi manque d'imposer le respect du principe de subsidiarité.

À travers la loi et le décret attaqué qui l'applique, les pouvoirs législatif et réglementaire proposent de répondre à ce critère de conventionnalité qu'est le respect du principe dit « de subsidiarité » : en principe, l'autorité administrative doit d'abord formuler une demande aux éditeurs ou aux hébergeurs du site visé de retrait du contenu en question ; ces derniers disposent de vingt-quatre heures pour se conformer à cette demande (article 6-1 de la LCEN et article 3 du décret attaqué) ; à défaut, injonction est faite aux fournisseurs d'accès de recourir à une mesure bien plus restrictive de liberté – notamment en raison des effets collatéraux de telles mesures – en bloquant l'accès au site.

Néanmoins, l'article 6-1, alinéa 2, de la LCEN dispose que le principe de subsidiarité peut ne pas être respecté lorsque :

> *« Toutefois, en l'absence de mise à disposition par la personne mentionnée au III du même article 6 des informations mentionnées à ce même III, l'autorité administrative peut procéder à la notification prévue à la première phrase du présent alinéa sans avoir préalablement demandé le retrait des contenus dans les conditions prévues à la première phrase du premier alinéa du présent article. »*

Les cas d'application du décret attaqué témoignent bien que des mesures alternatives pouvaient être adoptées. Dans le cas du site `islamic-news.info` par exemple, l'hébergeur était OVH une entreprise française et toutes les informations étaient disponibles en ligne pour identifier l'entreprise OVH comme telle ou encore pour identifier le détenteur du

nom de domaine. Une simple recherche sur un Whois[3] permet de s'en assurer.

En deuxième lieu, le décret ne permet pas à l'autorité administrative d'évaluer les techniques de blocage les plus adaptées aux finalités poursuivies, alors que la jurisprudence de la Cour EDH prévoit que l'autorité qui ordonne la mesure de blocage doit rechercher la mesure la moins lourde permettant de bloquer l'accès au site litigieux. Au lieu de cela, comme expliqué plus haut, le Gouvernement a fait le choix assumé d'encourager l'une des techniques de blocage comportant les effets collatéraux les plus importants.

En troisième lieu, en amont de la mesure de blocage, le décret attaqué échoue à prévoir un éventail des mesures suffisamment large pour permettre effectivement de parvenir au but poursuivi de la manière la plus proportionnée.

En particulier, il faudrait s'agissant des possibles alternatives au blocage distinguer les hébergeurs et éditeurs qui sont physiquement situés sur le territoire français et ceux situés à l'étranger.

Dans le premier cas, le Gouvernement ne justifie aucunement des difficultés d'application. Intervenir auprès de l'éditeur ou de l'hébergeur d'un site pour obtenir le retrait d'un contenu contrevenant aux articles 421-2-5 et 227-3 du code pénal ne requiert pas plus de difficultés que dans le cadre de la commission de quelconque autre infraction. Le blocage apparaît dans un tel cas totalement disproportionné.

Dans le second cas, lorsque les éditeurs ou les hébergeurs sont situés hors du territoire national, ni la loi ni le décret attaqué n'envisagent de passer par les voies de la coopération policière et judiciaire pour obtenir le retrait du contenu. Certes, le Gouvernement justifie la nécessité de recourir à des mesures de blocage de sites pour les internautes situés sur le territoire français par les lacunes et les lenteurs de la coopération policière et judiciaire internationale en matière de retrait de contenu. Mais les associations requérantes notent que ni la loi ni le décret attaqué ne prennent la peine d'opérer une distinction entre, d'une part, les éditeurs et hébergeurs qui échapperaient totalement aux autorités françaises car se situant dans des États non-coopératifs en matière de lutte contre la cybercriminalité et pour lesquels les demandes de retrait prononcées pourraient s'avérer inefficaces, de ceux qui, d'autre part, seraient situés sur le territoire français ou dans des États avec lesquels une coopération policière et judiciaire aurait toutes les chances d'aboutir. À titre d'exemple, les conventions d'entraide conclues par la France et l'Union européenne d'une part avec les États-Unis, d'autre part permettent d'obtenir de très nombreuses données d'identification et de connexion auprès des prestataires de services en ligne représentant une grande part du trafic Internet mondial. En ce sens, le décret n'engage pas l'autorité administrative à évaluer si, après une simple notification à l'éditeur ou l'hébergeur et avant le recours au blocage, une mesure moins lourde – par exemple le retrait du contenu via les mécanismes de coopération internationale – permettrait de parvenir à l'objectif poursuivi.

Compte tenu de la nature des infractions visées – la diffusion d'image de pornographie infantile et la provocation directe à des actes de terrorisme –, il semble non seulement possible mais surtout nécessaire d'approfondir la coopération pour lutter efficacement contre la diffusion de ces contenus dans le respect du droit international applicable. Force est de constater que les efforts diplomatiques en la matière se sont malheureusement taris.

[3]Base de données en ligne répertoriant les données associées à des noms de domaines, par exemple : `domaintools.com`.

La Convention du Conseil de l'Europe sur la cybercriminalité, en date de 2001 et qui se voulait un modèle en matière d'harmonisation des dispositions réprimant la criminalité informatique et cherchait à promouvoir une coopération internationale, se solde pour l'instant par un échec en raison du petit nombre de pays l'ayant ratifiée et des difficultés d'interprétation qu'elle génère. Ainsi, la Convention n'a été ratifiée que par les deux tiers du Conseil de l'Europe (ainsi des pays comme l'Irlande, la Suède ou la Russie ne l'ont pas ratifiée), et, à l'exception notable des États-Unis (qui y ont ajouté de nombreuses réserves d'interprétation), du Japon, de l'Australie, de l'Île Maurice et de la République dominicaine, par aucun État non-européen.

Avant d'arguer des lacunes de la coopération internationale pour justifier des mesures aussi restrictives de droit que le blocage de site Internet imposé aux opérateurs, le Gouvernement aurait dû faire la démonstration des efforts diplomatiques entrepris pour instaurer au niveau international un régime satisfaisant de coopération policière et judiciaire. Cette dernière permettrait en effet la mise en œuvre de la seule mesure efficace, à savoir le retrait des contenus des serveurs les hébergeant, pour empêcher les accès des internautes qui cherchant activement à accéder à ces contenus illicites.

Au lieu d'encourager la coopération internationale et de prévoir d'utiliser les mécanismes existants en la matière, le Gouvernement a donc préféré inscrire dans le droit français des mesures de blocage, dont des études montrent qu'elles ont pour effet de décourager le développement de la coopération internationale en matière de lutte contre la cybercriminalité.[4]

De plus, le décret autorise l'administration à faire, en amont des mesures de blocage, des demandes de retrait aux éditeurs ou aux hébergeurs étrangers et ce, sans aucune supervision judiciaire et en dehors des mécanismes de coopération internationale. Cela revient à prononcer unilatéralement une censure sur le territoire français d'informations provenant de pays tiers. Par ce décret, la France se déclare donc de fait en situation d'adopter une mesure de police dont les répercussions vont bien au-delà des frontières françaises et impacte par conséquent la liberté d'expression au-delà de ses frontières.

Enfin, pour ce qui est de l'objectif du Gouvernement d'empêcher l'accès par inadvertance des internautes français – en particulier les mineurs – à des contenus illicites et potentiellement traumatisants, le Gouvernement a également à sa disposition des mesures moins restrictives des droits et libertés fondamentaux et potentiellement plus efficaces : les filtres logiciels installés directement et volontairement par les internautes sur les terminaux informatiques et bloquant des contenus à l'aide d'une liste noire qui peut être abondée soit par des acteurs privés, associatifs ou publics. Il s'agit au demeurant d'un type d'outil dont la promotion permettrait de garantir un usage contrôlé de l'accès à Internet et qui, notamment dans la mesure où son utilisation relève du libre choix et de la responsabilité de la personne titulaire de l'accès Internet ou du propriétaire du poste informatique utilisé, est bien moins restrictive de liberté. Or, là encore, le Gouvernement ne démontre pas que ces mesures alternatives ont été sérieusement encouragées ni même simplement envisagées pour « prévenir l'accès involontaire des internautes français ».

[4] Moore, Tyler et Clayton, Richard, 2008. The Impact of Incentives on Notice and Take-down. In *Seventh Workshop on the Economics of Information Security (WEIS 2008)*. Disponible à l'adresse : `http://www.cl.cam.ac.uk/~rnc1/takedown.pdf`.

En conclusion,

Il existe des mesures alternatives moins restrictives de liberté que le blocage administratif de sites par nom de domaine pour parvenir aux objectifs poursuivis par le décret attaqué. Or, le Gouvernement n'a pas démontré le caractère irréalisable ou inefficace de ces mesures alternatives pour justifier le recours à une telle mesure. Le dispositif de blocage prévu dans le décret doit dès lors être déclaré non-nécessaire dans une société démocratique.

4.4. L'absence de contrôle juridictionnel viole les droits fondamentaux

4.4.1. La loi et le décret ne réunissent pas les garanties suffisantes pour éviter les abus

En droit,

La Convention EDH dispose dans son article 10 sauvegardant la liberté d'expression que :

> *« Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontière. Le présent article n'empêche pas les Etats de soumettre les entreprises de radiodiffusion, de cinéma ou de télévision à un régime d'autorisations.*
>
> *« L'exercice de ces libertés comportant des devoirs et des responsabilités peut être soumis à certaines formalités, conditions, restrictions ou sanctions prévues par la loi, qui constituent des mesures nécessaires, dans une société démocratique, à la sécurité nationale, à l'intégrité territoriale ou à la sûreté publique, à la défense de l'ordre et à la prévention du crime, à la protection de la santé ou de la morale, à la protection de la réputation ou des droits d'autrui, pour empêcher la divulgation d'informations confidentielles ou pour garantir l'autorité et l'impartialité du pouvoir judiciaire. »*

Suivant une jurisprudence constante de la Cour EDH, la liberté d'expression protégée inclut non seulement le droit de publier et d'éditer des contenus, mais elle implique aussi d'en protéger le corollaire que constitue la liberté du public d'accéder aux informations publiées (voir notamment *Observer & Guardian contre Royaume-Uni*, Cour EDH, Requête n° 13585/88 arrêt du 26 novembre 1991 § 59).

Dans l'arrêt *Yildrim c. Turquie* du 18 décembre 2012 déjà cité, la Cour EDH rappelle que les restrictions à cette liberté :

> *« doivent s'inscrire dans un cadre légal particulièrement strict quant à la délimitation de l'interdiction et efficace quant au contrôle juridictionnel contre les éventuels abus [...] (§ 64) »*

La Cour EDH a déjà eu l'occasion de se prononcer sur la nécessité d'avoir un cadre légal complet et précis encadrant les restrictions apportées à la liberté d'expression par l'autorité administrative.

Ainsi, dans l'arrêt du 17 juillet 2001, *Association Ekin contre France* n° 39288/98 la Cour rappelle que de telles restrictions présentent « de si grands dangers qu'elles appellent de la part de la Cour l'examen le plus scrupuleux » (§ 56).

Dans cette affaire, les dispositions en cause étaient celles du décret-loi du 6 mai 1939 relatif au contrôle de la presse étrangère, lequel conférait au ministre de l'intérieur « de vastes prérogatives en matière d'interdiction administrative de diffusion de publications de provenance étrangère ou rédigées en langue étrangère ».

Le décret-loi prévoyait pourtant un contrôle juridictionnel des décisions publiques de l'administration, mais sans pour autant apporter des garanties suffisantes. Sans équivoque, la Cour en tire la conséquence que :

> *« S'agissant des modalités et de l'étendue du contrôle juridictionnel de la mesure administrative d'interdiction, la Cour constate que le contrôle juridictionnel intervient a posteriori. En outre, ce contrôle n'est pas automatique, la procédure de contrôle par le juge ne s'enclenchant que sur recours de l'éditeur. [...] Enfin, d'après l'article 8 du décret du 28 novembre 1983, dès lors que l'administration invoque le caractère urgent de la mesure, l'éditeur n'a pas la possibilité de présenter, préalablement à l'adoption de l'arrêté d'interdiction, ses observations orales ou écrites. Tel fut bien le cas en l'espèce. En conclusion, la Cour estime que le contrôle juridictionnel existant en matière d'interdiction administrative de publications ne réunit pas des garanties suffisantes pour éviter les abus. » (§ 61)*

Ainsi, ne réunit pas des garanties suffisantes pour éviter les abus, et est contraire à la Convention EDH, la mesure de censure que peut prononcer l'administration sans être précédée ni d'un contrôle juridictionnel ni de la possibilité pour l'éditeur du contenu censuré de présenter ses observations.

En l'espèce,

L'article 6-1 de la LCEN permet à l'autorité administrative d'enjoindre les fournisseurs d'accès à Internet à bloquer des contenus publiés au moyen d'un service de communication au public en ligne. Cette mesure constitue une restriction de la liberté d'expression de l'éditeur du contenu dont la publication est ainsi censurée, mais aussi du droit du public à accéder au service.

Qu'en est-il des garanties qui entourent cette mesure de censure afin d'en éviter les abus ?

D'abord, l'article 6-1 alinéa 1 de la LCEN prévoit que :

> *« [...] l'autorité administrative peut demander à toute personne mentionnée au III de l'article 6 de la présente loi **ou** aux personnes mentionnées au 2 du I du même article 6 de retirer les contenus qui contreviennent à ces mêmes articles 421-2-5 et 227-23. »*

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

Il résulte ainsi de l'article 6-1 alinéa 1 précité que l'administration peut choisir de ne prévenir que l'hébergeur d'un service avant d'en exiger le blocage, ce qui dispense l'administration de systématiquement prévenir l'éditeur des contenus.

Ce faisant, l'éditeur serait privé de la possibilité de présenter ses observations préalablement à la mesure de blocage.

Ensuite, l'article 6-1 alinéa 2 prévoit que :

> *« Toutefois, en l'absence de mise à disposition par la personne mentionnée au III du même article 6 des informations mentionnées à ce même III, l'autorité administrative peut procéder à la notification prévue à la première phrase du présent alinéa sans avoir préalablement demandé le retrait des contenus dans les conditions prévues à la première phrase du premier alinéa du présent article. »*

Le III de l'article 6 de la LCEN prévoit que les éditeurs de service ont l'obligation de mettre à disposition du public, s'ils sont des personnes physiques, « leurs nom, prénoms, domicile et numéro de téléphone » ou, s'ils sont des personnes morales, « leur dénomination ou leur raison sociale et leur siège social, leur numéro de téléphone » ou seulement, s'ils éditent leur service à titre non professionnel, « le nom, la dénomination ou la raison sociale et l'adresse » de l'hébergeur de leur service et à condition d'avoir transmis à ce dernier les informations précédantes les concernant.

Il apparaît donc que pour tout service ne présentant pas ces mentions en bonne et due forme (ce qui est le cas de nombre de sites Web, notamment de la majorité des sites non professionnels), l'autorité administrative peut enjoindre les fournisseurs d'accès à Internet à le bloquer alors même que ni son hébergeur ni son éditeur n'a été prévenu.

Or, il est tout à fait possible pour l'autorité administrative de notifier les hébergeurs ou éditeurs quand bien même les informations obligatoires du III de l'article 6 de la LCEN ne sont pas mentionnées. À titre d'exemple, parmi les services de communication au public en ligne ayant fait l'objet d'une mesure de blocage ordonnée par l'autorité administrative, la plupart étaient hébergés par des personnes morales facilement identifiables, lesquelles auraient été en mesure de transférer la notification à l'éditeur du contenu en cause.

Ainsi, si un service ne présente pas ces mentions obligatoires, ni son éditeur ni son hébergeur ne pourraient présenter leurs observations préalablement au blocage du service, alors même que l'absence de ces mentions ne saurait justifier l'impossiblité pour l'administration de les en informer préalablement.

Dans ces deux cas, ce défaut d'information nuit d'autant plus à la possibilité de l'éditeur de faire valoir ses observations que, contrairement à l'arrêt *association Ekin contre France* qui concernait des arrêtés d'interdiction, en l'espèce, les décisions de l'autorité administrative ne sont pas notifiées au public.

Enfin, l'article 6-1 de la LCEN n'exige aucun contrôle juridictionnel préalable aux

mesures de censure qu'il autorise.

En conclusion,

Les dispositions de l'article 6-1 de la LCEN et du décret attaqué qui en résulte échouent à apporter les moindres garanties contre les abus, exigées par la Cour EDH, en autorisant l'administration à prendre des mesures portant atteinte à la liberté d'expression sans être précédées ni d'un contrôle juridictionnel ni de la possibilité pour l'éditeur du contenu censuré de présenter ses observations.

Ceci est d'autant plus préoccupant que les contenus pouvant faire l'objet d'un blocage ordonné par l'administration sont notamment les contenus contrevenant à l'article 421-2-5 du code pénal qui incrimine le fait de provoquer directement à des actes de terrorisme ou de faire publiquement l'apologie de ces actes. Or, il est indéniable que la qualification des actes relevant de cet article est périlleuse, tant les définitions d'« apologie » ou de « terrorisme » sont floues.

On peut ainsi constater que le site `islamic-news.info` qui a fait l'objet d'une mesure de blocage au titre de l'article 6-1 de la LCEN a été censuré parce qu'il reproduisait un discours du leader de l'État Islamique « sans le mettre en perspective » selon le ministère de l'intérieur[5].

Il est tout à fait discutable que l'absence de mise en perspective puisse être considérée comme relevant de l'apologie ou de la provocation, ce qui témoigne de l'impérieuse nécessité que les mesures de blocage fassent l'objet d'un débat contradictoire garanti par une autorité impartiale et indépendante et que l'éditeur ait la possibilité de contester ces allégations.

Par conséquent, les requérants demandent au Conseil d'État d'évincer l'article 6-1 de la LCEN en ce qu'il est contraire à l'article 10 de la Convention EDH et d'en déduire l'annulation du décret attaqué.

4.4.2. Les voies de recours a posteriori sont ineffectives

En droit,

La Convention EDH, en son article 6, paragraphe 1 relatif au droit à un procès équitable, dispose que :

> *« Toute personne a droit à ce que sa cause soit entendue équitablement, publiquement et dans un délai raisonnable, par un tribunal indépendant et impartial, établi par la loi, qui décidera, soit des contestations sur ses droits et obligations de caractère civil, soit du bien-fondé de toute accusation en matière pénale dirigée contre elle. [...] »*

[5] « Les ratés de la première vague de blocages administratifs de sites djihadistes », *LeMonde.fr*, 18 mars 2015. Article accessible à l'adresse : `http://www.lemonde.fr/pixels/article/2015/03/18/les-rates-de-la-premiere-vague-de-blocages-administratifs-de-sites-djihadistes_4596149_4408996.html`

Tel qu'interprété par la Cour EDH, l'article 6, paragraphe 1, de la Convention EDH implique le respect du principe d'égalité des armes entre les parties.

Dans l'arrêt *Hentrich contre France* requête n° 13616/88 du 22 septembre 1994, la Cour EDH a eu l'occasion de rappeler que :

> *« une des exigences d'un « procès équitable » est « l'égalité des armes », laquelle implique l'obligation d'offrir à chaque partie une possibilité raisonnable de présenter sa cause dans des conditions qui ne la placent pas dans une situation de net désavantage par rapport à son adversaire (voir l'arrêt Dombo Beheer B.V. c. Pays-Bas du 27 octobre 1993, série A no 274, p. 19, par. 33). Or en l'espèce la procédure sur le fond n'a pas offert à la requérante une telle possibilité : d'un côté, les juges du fond ont permis à l'administration de se borner à motiver sa décision d'exercice du droit de préemption en qualifiant d'« insuffisant le prix de cession déclaré dans l'acte » (paragraphes 9 et 15 ci-dessus), motivation trop sommaire et générale pour permettre à Mme Hentrich de présenter une contestation raisonnée de cette appréciation ; de l'autre, les juges du fond n'ont pas voulu permettre à la requérante d'établir que le prix convenu entre les parties correspondait à la valeur vénale réelle du bien.*
>
> *« Il y a donc eu violation de l'article 6 par. 1 (art. 6-1) sur ce point. »*

En l'espèce,

L'article 2 du décret attaqué dispose que :

> *« La liste des adresses électroniques des services de communication au public en ligne* ***contrevenant aux articles 227-23 et 421-2-5 du code pénal*** *est adressée aux personnes mentionnées au 1 du I de l'article 6 de la loi du 21 juin 2004 susvisée selon un mode de transmission sécurisé, qui en garantit la confidentialité et l'intégrité. »*

La mesure de blocage requise par l'administration auprès du fournisseur d'accès à Internet est constitutive d'une accusation en matière pénale dirigée notamment contre l'éditeur du service bloqué. En effet, en ordonnant le blocage l'administration qualifie le service en cause comme étant constitutif des faits matériels incriminés par les articles 227-23 et 421-2-5 du code pénal.

L'article 6, paragraphe 1, de la Convention EDH est donc bien applicable et l'éditeur est en droit de bénéficier des droits émanant de cet article.

Or, il s'avère qu'en l'espèce ce droit au procès équitable est ineffectif.

L'article 3 du décret attaqué dispose que :

> *« Dans un délai de vingt-quatre heures suivant la notification prévue au deuxième alinéa de l'article 6-1 de la loi du 21 juin 2004 susvisée, les personnes mentionnées au 1 du I de l'article 6 de la même loi empêchent par tout moyen approprié l'accès aux services fournis par les adresses électroniques figurant sur la liste et le transfert vers ces services.*
>
> *« Elles ne peuvent pas modifier la liste, que ce soit par ajout, suppression ou altération.*

« Elles préservent la confidentialité des données qui leur sont ainsi confiées. »

Dans le dispositif de blocage institué par l'article 6-1 de la LCEN et le décret attaqué, la liste des adresses électroniques bloquées est secrète. Aucune mesure de publication ni de notification n'est prévue. La décision de blocage ne consiste en fait qu'en l'ajout d'une adresse électronique sur une liste transmise aux fournisseurs d'accès à Internet.

Les recours contentieux qui peuvent être envisagés contre cette décision, constitutive d'une accusation en matière pénale ne peuvent être initiés que dans la méconnaissance des motifs qui ont conduit à l'adoption de cette décision. Il en va de même du recours contre le refus de l'administration d'abroger la mesure de blocage, cette décision de refus pouvant très bien être implicite, puisqu'en la matière le silence de l'administration vaut rejet.

Ainsi, les éditeurs de services ayant fait l'objet d'une mesure de blocage ne disposent d'aucune information relative aux motifs propres à leur situation ayant conduit l'administration à prendre cette décision.

Les éditeurs de services doivent donc initier une action juridictionnelle contre une décision dont ils ignorent tant les motifs que la portée, puisqu'il s'avère que l'ensemble d'un site peut être bloqué alors que seulement certaines de ses pages ou contenus seraient en cause.

Cette situation crée *ab initio* une inéquité entre les parties au procès puisque le demandeur ne peut motiver sa demande d'annulation de la décision administrative attaquée.

Cette situation diffère de toutes celles connues en droit. Jusqu'à ce jour, concernant les services de communication au public en ligne, n'étaient connues que des mesures de blocage judiciaires. Lorsqu'une mesure de blocage est demandée auprès d'une juridiction, la partie demanderesse est nécessairement tenue de justifier sa demande. Cela vaut tant dans les cas où, par exemple un ayant-droit ou l'administration demandent le blocage d'un site.

Aussi, en droit de la presse où en vertu de l'article 53 de la loi du 29 juillet 1881, les faits incriminés doivent être précisés et qualifiés dès la citation tout autant que la loi applicable doit y être indiquée.

Ces cas témoignent du fait qu'avant l'adoption du décret attaqué, le principe de l'égalité des armes était, en principe, préservé à travers le procès.

En conclusion,

L'absence de décision motivée de l'administration viole l'article 6, paragraphe 1, de la Convention EDH en ce qu'elle entrave le principe de l'égalité des armes entre les parties au procès, rendant le droit au procès équitable ineffectif.

Dès lors, le décret attaqué doit être annulé.

4.4.3. Le contrôle des mesures par une personne qualifiée de la CNIL est ineffectif

L'article 6-1 de la LCEN dispose que :

> *« L'autorité administrative transmet les demandes de retrait et la liste mentionnées, respectivement, aux premier et deuxième alinéas à une personnalité qualifiée, désignée en son sein par la Commission nationale de l'informatique et des libertés pour la durée de son mandat dans cette commission. Elle ne peut être désignée parmi les personnes mentionnées au 1° du I de l'article 13 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. La personnalité qualifiée s'assure de la régularité des demandes de retrait et des conditions d'établissement, de mise à jour, de communication et d'utilisation de la liste. Si elle constate une irrégularité, elle peut à tout moment recommander à l'autorité administrative d'y mettre fin. Si l'autorité administrative ne suit pas cette recommandation, la personnalité qualifiée peut saisir la juridiction administrative compétente, en référé ou sur requête. »*

La personnalité qualifiée a été nommée par une délibération de la CNIL du 29 janvier 2015 en la personne de M. Alexandre Linden (Délibération n° 2015-056 du 29 janvier 2015 portant désignation par la Commission nationale de l'informatique et des libertés de la personnalité qualifiée prévue par l'article 6-1 de la loi pour la confiance dans l'économie numérique).

Cette personne devra pouvoir bénéficier de l'appui des services de l'autorité.

Or, s'il s'agit de contrôler la mise en œuvre et la pertinence du blocage d'adresses électroniques préalablement identifiées ainsi que leur transfert, il s'agit là d'une fonction qui peut être cumulée avec celles de membre de la CNIL sans qu'il soit prévu un encadrement approprié. Comme la CNIL a pu l'observer dans son avis, si le contrôle opéré par la personnalité qualifiée doit être effectif alors elle doit disposer de moyens à la mesure de sa mission.

Qui plus est, comme la CNIL a là encore pu le relever, compte tenu de la nature sensible des données en cause, il convenait d'introduire un mécanisme assurant la protection de l'ensemble des données qu'il aura à traiter. Or il n'en est rien.

De ce fait, la décision attaquée porte une atteinte disproportionnée aux droits fondamentaux mis en cause et devra être annulée.

4.5. L'interception des communications vers les sites bloqués est illégale

Si par extraordinaire le Conseil d'État reconnaissait le pouvoir réglementaire compétent pour instituer l'atteinte aux droits et libertés fondamentaux portée par l'article 3, alinéa 4 (cf. *supra* page 13) alors, la légalité de cette disposition devrait être examinée au regard des règles de droit qu'il doit respecter.

L'article 3, alinéa 4, du décret attaqué devrait alors être annulé en ce qu'il est contraire

à l'article L. 34-1 du CPCE qui organise la conservation des données à caractère personnel par les opérateurs de communications életroniques et la transmission de ces données aux autorités.

L'article 3, alinéa 4, devrait également être annulé en ce qu'il enfreint, d'une part, la loi Informatique, fichiers et libertés du 6 janvier 1978 et porte une atteinte disproportionnée, d'autre part, aux droits et libertés fondamentaux que sont la liberté d'expression, la liberté d'entreprendre, la protection de la vie privée et la protection des données personnelles.

4.5.1. Le transfert de données que constitue la redirection depuis les services bloqués est illégal

En droit,

La loi impose aux opérateurs de communications électroniques d'effacer ou d'anonymiser toute donnée à caractère personnel qu'ils sont amenés à traiter dans le cadre de leur activité.

L'article L34-1, I, du code des postes et des communications électroniques (CPCE) définit ainsi le champ de cette obligation :

> *« I.-Le présent article s'applique au traitement des données à caractère personnel dans le cadre de la fourniture au public de services de communications électroniques ;*

Un traitement de données à caractère personnel étant toute opération réalisée sur de telles données, sont donc concernés les transferts de toutes données à caractère personnel qu'un opérateur est conduit à appréhender dans le cadre de la fourniture de ses services au public.

L'article L34-1, II, définit ainsi l'obligation d'effacement à laquelle les opérateurs sont tenus quant à ces données :

> *« 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. »*

Les opérateurs ont donc, en principe, l'obligation de ne transférer aucune donnée permettant d'identifier l'auteur des communications dont ils ont la charge. Mais les dispositions des III, IV, V et VI du même article prévoient en effet différentes exceptions à cette obligation d'effacement, notamment en permettant de le différer pour « les besoins de la recherche, de la constatation et de la poursuite des infractions pénales ». Or, l'article L. 34-1, VI, CPCE limite précisément le champ de ces exceptions en disposant que :

> *« Les données conservées et traitées dans les conditions définies aux III, IV et V 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.*

> *« **Elles ne peuvent en aucun cas porter sur** le contenu des correspondances échangées ou **des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications.** »*

Ainsi, les opérateurs ont l'obligation, sans exception, de ne transférer aucune donnée permettant d'identifier l'auteur de communications et révélant les « informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications ».

En l'espèce,

L'article 3, alinéa 4, du décret attaqué dispose que :

> *« Les utilisateurs des services de communication au public en ligne auxquels l'accès est empêché sont dirigés vers une page d'information du ministère de l'intérieur, indiquant pour chacun des deux cas de blocage les motifs de la mesure de protection et les voies de recours. »*

Cette disposition, qui n'est pas prévue par la loi, oblige les fournisseurs d'accès à Internet à rediriger les connexions tentant d'atteindre un service dont l'accès est empêché vers une page d'information du ministère de l'intérieur.

Lors de cette opération, de nombreuses données à caractère personnel concernant les personnes à l'origine de ces connexions sont automatiquement transmises au service du ministère de l'intérieur hébergeant cette page d'information. Parmi ces données figurent au moins l'adresse IP du terminal de ces personnes, permettant de les identifier, et l'adresse du site bloqué qu'elles ont consulté et depuis lequel elles ont été redirigées vers la page d'information.

Ce faisant, cette obligation impose aux opérateurs de transférer des données permettant d'identifier l'auteur des communications en cause et révélant les « informations consultées [...] dans le cadre de ces communications ».

En conclusion,

L'article 3, alinéa 4, du décret attaqué crée une disposition, non prévue par la loi, qui oblige les opérateurs à faire ce que l'article L34-1 du CPCE leur interdit.

En conséquence, l'article 3, alinéa 4, du décret attaqué, contraire à la loi, doit être annulé.

4.5.2. La collecte de données résultant de la redirection depuis les services bloqués est illégale

En droit,

L'article 6 de la loi du 6 janvier 1978 dispose que :

« Un traitement ne peut porter que sur des données à caractère personnel qui satisfont aux conditions suivantes :

« 1° Les données sont collectées et traitées de manière loyale et licite ;

« 2° Elles sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités. Toutefois, un traitement ultérieur de données à des fins statistiques ou à des fins de recherche scientifique ou historique est considéré comme compatible avec les finalités initiales de la collecte des données, s'il est réalisé dans le respect des principes et des procédures prévus au présent chapitre, au chapitre IV et à la section 1 du chapitre V ainsi qu'aux chapitres IX et X et s'il n'est pas utilisé pour prendre des décisions à l'égard des personnes concernées ;

« 3° Elles sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs ;

« 4° Elles sont exactes, complètes et, si nécessaire, mises à jour ; les mesures appropriées doivent être prises pour que les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées soient effacées ou rectifiées ;

« 5° Elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées. »

En l'espèce,

Comme énoncé précédemment, l'article 3, alinéa 4, du décret attaqué autorise la collecte des données à caractère personnel par le ministère de l'intérieur.

Pour autant, le décret ne lui associe aucune finalité, violant de ce chef l'article 6, point 2°, précité.

A fortiori, les données collectées ne peuvent être jugées adéquates, pertinentes et non excessives à l'égard d'aucune finalité, en violation du 3° de ce même article.

Enfin, le décret ne prévoit aucune durée de conservation des ces données ni de procédure d'effacement, en violation du 5° de ce même article.

En conclusion,

Le présent décret, en son article 3, alinéa 4, viole l'article 6 de la loi du 6 janvier 1978.

4.5.3. La redirection depuis les services bloqués porte une atteinte disproportionnée aux droits et libertés fondamentaux

Comme cela a été observé page 13, l'article 3 alinéa 4 du décret attaqué impose aux fournisseurs d'accès à Internet de rediriger leurs utilisateurs vers une page du ministère de l'intérieur, ce qui implique que des données personnelles identifiant les utilisateurs

ayant tenté d'accéder à un service dont l'accès est empêché sont envoyées au ministère de l'intérieur.

4.5.3.1. Les atteintes aux libertés constituées par l'article 3, alinéa 4, du décret attaqué

Constitue une entrave déterminante pour les fournisseurs d'accès à Internet le fait de devoir se faire le relais d'une dénonciation de leurs abonnés au ministère de l'intérieur.

Et constitue une atteinte grave à la vie privée et à la protection des données personnelles le simple fait d'obliger un fournisseur d'accès à Internet de transmettre au ministère de l'intérieur les données personnelles de ses abonnés.

Par ailleurs, la CJUE rappelle que permettre l'accès des autorités nationales à des données de connexion est une atteinte aux libertés :

> *« En imposant la conservation des données énumérées à l'article 5, paragraphe 1, de la directive 2006/24 et en permettant l'accès des autorités nationales compétentes à celles-ci, cette directive déroge, ainsi que l'a relevé M. l'avocat général notamment aux points 39 et 40 de ses conclusions, au régime de protection du droit au respect de la vie privée, instauré par les directives 95/46 et 2002/58, à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques, ces dernières directives ayant prévu la confidentialité des communications et des données relatives au trafic ainsi que l'obligation d'effacer ou de rendre anonymes ces données lorsqu'elles ne sont plus nécessaires à la transmission d'une communication, hormis si elles sont nécessaires à la facturation et uniquement tant que cette nécessité perdure. »*
> *(CJUE, arrêt du 8 avril 2014, Digital Rights Ireland, C-293-12, § 32)*
>
> *« En outre, l'accès des autorités nationales compétentes aux données en question constitue une ingérence supplémentaire dans ce droit fondamental (voir, en ce qui concerne l'article 8 de la CEDH, arrêts Cour EDH, Leander c. Suède, 26 mars 1987, série A n°116, § 48 ; Rotaru c. Roumanie [GC], n° 28341/95, § 46, CEDH 2000-V, ainsi que Weber et Saravia c. Allemagne (déc.), n° 54934/00, § 79, CEDH 2006-XI). Ainsi, les articles 4 et 8 de la directive 2006/24 prévoyant des règles relatives à l'accès des autorités nationales compétentes aux données sont également constitutifs d'une ingérence dans les droits garantis par l'article 7 de la Charte. »*
> *(idem, § 35)*

Dès lors, cette atteinte aux libertés doit être prévue par la loi, être nécessaire et proportionnée.

4.5.3.2. Il existe des solutions alternatives

Une solution alternative est possible, plus protectrice des libertés, apportant les mêmes informations à l'internaute bloqué, et compatible avec le texte de la loi n° 2014-1353 précitée : les pages d'information pourraient être transmises aux fournisseurs d'accès à Internet par le ministère de l'intérieur, charge aux fournisseurs d'accès à Internet d'afficher ces pages aux internautes essayant d'accéder à un site bloqué.

C'est cette solution alternative qui est mise en place par la fournisseurs d'accès concernés dans les cas actuels de blocage de sites web suite à une décision de justice.

Le seul motif qui pourrait justifier l'utilisation de la solution proposée par le décret attaqué est *la volonté que ces informations personnelles soient transmises aux pouvoirs publics*. La dangerosité de ce dispositif est mentionnée par la CNIL dans son avis quand elle indique[6] :

> *« En cinquième lieu, s'agissant des modalités d'information des internautes des services de communication au public en ligne faisant l'objet d'une mesure de blocage, l'article 3 du projet de décret prévoit qu'ils seront dirigés vers une page d'information du ministère de l'intérieur indiquant, pour chacun des deux cas de blocage, les motifs de la mesure de protection et les voies de recours.*
>
> *« A cet égard, la commission relève que le cadre juridique actuel ne permet ni la collecte ni l'exploitation, par l'OCLCTIC, des données de connexion des internautes qui seraient redirigés vers la page d'information du ministère de l'intérieur. Elle rappelle que si des traitements de données à caractère personnel spécifiques étaient alimentés par ces données, ils devraient être soumis à l'examen préalable de la commission. »*
>
> *(Délibération n° 2015-001, du 15 janvier 2015, publiée au JORF numéro 39 du 15 février 2015, texte n° 65)*

La CNIL a donc déjà clairement identifié les données concernées comme étant des données à caractère personnel et identifie spécifiquement la collecte et le traitement de ces données comme un risque d'excès de pouvoir de l'autorité administrative.

En conséquence, l'article 3, alinéa 4, du décret attaqué devra être annulé.

[6] Texte annexé à la présente.

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

1. Annule le décret attaqué avec toutes conséquences de droit ;

2. 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 29 mars, à Paris

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

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

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

Pièces produites

1. Décret n° 2015-125 du 5 février 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique, publié au JORF n° 0031 du 6 février 2015, page 1811.
2. Commission Nationale de l'informatique et des libertés : Délibération n° 2015-001 du 15 janvier 2015 portant avis sur un projet de décret relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pédopornographique (demande d'avis n° 14037041), publié au JORF n° 39 du 15 février 2015.
3. Statuts de l'association French Data Network.
4. Extrait du compte rendu de la réunion du bureau de FDN du 7 mars 2015 donnant pouvoir au président.
5. Statuts de l'association La Quadrature du Net.
6. Extrait du compte rendu de la consultation du Bureau de La Quadrature du Net du 29 mars 2015, donnant pouvoir au président.
7. Statuts de la Fédération des fournisseurs d'accès à Internet associatifs, dite Fédération FDN.
8. Charte de la Fédération FDN.
9. Compte rendu de la réunion du bureau de la Fédération FDN du 16 mars 2015 donnant pouvoir au président.
10. La présente requête.

L'ensemble étant produit en 6 exemplaires.