Conseil d'État
Section du contentieux
N° 389140

Mémoire en réplique

PRODUIT PAR

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

CONTRE

Le 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° 31 du 6 février 2015, page 1811

I. LÉGALITÉ EXTERNE

Les associations requérantes soulèvent que l'obligation de redirection des internautes vers une page du ministère de l'intérieur constitue une atteinte à la liberté de communication et au secret des correspondances non prévue par la loi ainsi qu'un violation des dispositions de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

En défense, le Gouvernement argue que l'obligation de redirection est une stricte modalité d'application de la mesure de blocage (section 1) et que les données ainsi traitées n'ont pas de caractère personnel (section 2 page 3). Ce que les associations requérantes contestent.

1. La redirection n'est pas une modalité d'exécution du blocage

Les associations requérantes soutiennent que la redirection des internautes vers une page du ministère de l'intérieur n'est pas prévue par la loi. Le Gouvernement allègue en réponse qu'« il était nécessaire de rediriger l'internaute vers une page – c'est la conséquence du blocage ».

Or, **premièrement**, cette affirmation est fausse sur un plan technique. Tout d'abord, le blocage peut fonctionner sans qu'aucune redirection n'ait lieu (par exemple, en falsifiant les réponses du serveur DNS aux requêtes des adresses électroniques visées en renvoyant une adresse IP locale, ou en renvoyant une erreur indiquant que le domaine n'existe pas [1]). Le Gouvernement l'indique clairement : « la réponse [peut] être au minimum un message d'erreur » (p. 4).

Deuxièmement, si le Gouvernement souhaitait qu'une page d'information s'affiche aux internautes lorsqu'ils tentent d'accéder aux adresses électroniques visées, il n'était nullement nécessaire pour cela que la redirection se fasse vers une page hébergée sur un serveur du ministère de l'intérieur. En effet, de telles pages d'information pourraient par exemple être stockées en local sur le boîtier de connexion fourni par le fournisseur d'accès à internet.

Sur ce point précis, le Gouvernement prétend que rediriger les internautes vers une page hébergée par ces opérateurs les exposerait à des cyberattaques présentant pour eux

1. C'est par exemple le message d'erreur qu'on obtient quand on tente d'accéder à un domaine qui n'existe pas dans un navigateur Web

un risque de faillir à leurs obligations de permanence, de disponibilité, de sécurité et d'intégrité du réseau, et qu'ils se seraient ainsi eux-mêmes opposés à cette option.

Néanmoins, il est en pratique peu réaliste de prétendre qu'ils s'y soient opposés par crainte que ces attaques présentent peur eux un tel risque. Les attaques par déni de service sont en effet un problème relativement courant sur le réseau. Il s'en produit tout le temps, partout dans le monde, pour un nombre très varié de motifs. La gestion des attaques de ce type est en général faite par les opérateurs du réseau, que ce soient les opérateurs de transport, les hébergeurs, ou les fournisseurs d'accès.

La question ne peut donc pas être une question de connaissances techniques : on peut légitimement supposer que les équipes d'ingénierie des grands fournisseurs d'accès comptent plus de spécialistes du réseau qu'une administration dont ce n'est pas le métier principal. Il n'est alors question que d'une inversion de responsabilité et de coûts, les FAI ne souhaitent pas être responsables du bon fonctionnement d'un système dont la maintenance pourrait être délicate.

Techniquement peu réaliste, ce n'est, en tout état de cause, pas un argument de nature à permettre une atteinte aux libertés qui ne soit pas prévue par la loi. Il démontre cependant qu'**une autre solution était possible, portant moins atteinte aux libertés.**

Car, **troisièmement**, sur un plan juridique, la redirection n'est pas non plus requise par la loi. Par exemple, l'affichage d'un message d'erreur est la solution retenue par défaut pour les sites bloqués au titre de la loi n° 2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne. En pratique, les noms de domaines bloqués au titre de l'article 61 de cette loi ne renvoient vers aucune page d'information [2]. Étant observé que l'article 61 de la loi du 12 mai 2010 et l'article 6-1 de la LCEN ne se distinguent en rien à cet égard : aucun des deux articles n'impose de redirection vers une page quelconque. Pourtant les deux procédures divergent. Et si elles divergent ce n'est pas en raison d'une des deux lois mais par la volonté du pouvoir réglementaire, exprimée en l'espèce à travers le décret attaqué.

Quatrièmement, le Gouvernement avance que le recours à cette page d'information se fonde sur l'article 25, paragraphe 2 de la directive 2011/92/UE qui exige que le blocage soit établi « par le biais de procédures transparentes ». À aucun moment la page d'information du ministère n'a permis d'accomplir cet objectif de transparence : ni l'auteur du site, ni son hébergeur, ni le lecteur de la page d'information ne savent ce qui est reproché à quel contenu relevant du site bloqué et ne peuvent en aucune manière connaître ni les motifs du blocage ou l'état de la procédure conduisant l'administration vers sa décision de blocage.

Il faut aussi noter que c'est au contraire l'opacité qui marque les mesures choisies, la liste des adresses bloquées étant tenue secrète tant aux internautes qu'aux personnes directements concernées – seule la tentative d'accès à un site bloqué révélant telle circonstance. De même, l'application concrète du présent décret est en contradiction avec l'intention de transparence que se prête ici le Gouvernement, la « page d'information » vers laquelle il avait choisi de rediriger les internautes ne donnant d'information ni sur le contenu précis ayant provoqué le blocage – parmi la multitude de contenus susceptibles

2. Voir les conséquences des ordonnances du 30 janvier 2015 du tribunal de grande instance de Paris prises dans les affaires 14/61086, 14/61087, 14/61088, 14/61091 et 14/61092 concernant respectivement les sites etopaz.az, casinonoir.com, lucky31.com, casinolariviera.com, maximuscasino.com

d'être présents sur le site bloqué –, ni sur les motivations propres à l'espèce de ce blocage, ni sur l'état de la procédure y ayant conduit. Aucune décision publique ou aucun portail n'informe par ailleurs précisément et clairement sur ces mesures.

Qui plus est, puisque la liste des sites bloqués est maintenue secrète, il n'est pas possible de savoir à ce jour si le Gouvernement procède toujours à l'affichage d'une page d'information alors qu'il est apparu que celle-ci n'avait plus cours [3].

À l'inverse, pour ce qui concerne les sites de jeux et paris en ligne bloqués par décision du tribunal de grande instance de Paris, une recherche sur le site de l'ARJEL ainsi qu'une recherche de jurisprudence permettent au moins de savoir quels sites ont été bloqués et pour quel motif (en l'occurence, l'absence d'agrément préalable de l'ARJEL). Qui plus est, l'information sur les dispositifs légaux et illégaux de paris en ligne n'en est pas moins faite, en l'absence d'une redirection vers une page hébergée par le ministère de l'intérieur, que ce soit à travers des campagnes publiques d'information, le site de l'ARJEL ou encore les décisions de justice imposant les mesures de blocage.

En conclusion, il apparaît que la redirection vers un site du ministère de l'intérieur est une mesure qui n'est pas qu'une modalité d'exécution de la loi mais une décision propre à l'administration dont l'utilité n'a d'ailleurs pas encore été démontrée. À l'inverse, comme cela a été démontré dans la requête introductive et vainement contesté par le Gouvernement, cette redirection emporte, la violation de l'article 34 de la Constitution, des atteintes disproportionnées à des droits et libertés fondamentaux ainsi que plusieurs illégalités.

2. Le caractère personnel des données traitées

Le ministère de l'Intérieur allègue que les données qui lui sont transmises, lorsque des internautes se rendent sur un site bloqué et sont dirigés vers la page d'infomation du ministère de l'intérieur, ne sont « qu'indirectement des données personnelles » car elles ne pourraient acquérir ce caractère « que du rapprochement des adresses IP avec l'identité des internautes au travers du traitement de données mis en œuvre par chaque FAI ».

Pourtant, la redirection des internautes vers la page d'information hébergée sur un serveur du ministère de l'intérieur implique bien la transmission d'une somme de données non négligeable, consititutives de données personnelles et, partant, la réalisation d'un traitement de données à caractère personnel illicite en l'état.

En droit, une donnée acquiert un caractère personnel notamment lorsqu'elle est relative à une personne physique pouvant être identifiée, même indirectement. D'après les termes de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés :

> *Article 2*
> *« [...] Constitue une donnée à caractère personnel toute information relative à une per-*

3. La page d'information alors affichée au début de la mise en œuvre du dispositif n'est pas apparue comme une solution pérenne.

Voir Fradin, A., « « The Voice » et la main rouge : l'Intérieur se prend les pieds dans la com' », *Rue89.nouvelobs.com*, 16 mars 2015 ; et Fradin, A., « La « main rouge » affichée sur les sites bloqués va disparaître », *Rue89.nouvelobs.com*, 18 mars 2015.

sonne physique ***identifiée ou qui peut être identifiée, directement ou indirectement****, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne.*

« Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, 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. [...] »

En 2007, le Groupe de travail de l'article 29 a précisé ce que recouvrait l'exigence selon laquelle la donnée personnelle doit se rapporter à une personne identifiée ou identifiable :

> « De plus amples explications se trouvent dans le commentaire sur les articles de la proposition modifiée de la Commission, en ce sens qu'il y est précisé qu'« une personne peut être identifiée soit directement par un nom soit indirectement par un numéro de téléphone, de voiture, de sécurité sociale, de passeport ou par un croisement de critères significatifs, permettant de la reconnaître à l'intérieur d'un petit groupe par exemple (âge, fonction occupée, adresse, etc.) ». Ce libellé montre clairement que c'est **le contexte du cas d'espèce** qui déterminera si certains identifiants sont suffisants pour permettre l'identification. Un nom de famille très courant sera insuffisant pour identifier quelqu'un — c'est-à-dire pour distinguer quelqu'un — dans l'ensemble de la population d'un pays, alors qu'il sera probablement suffisant pour identifier un élève dans une classe. Même des informations accessoires, comme « l'homme portant un costume noir » peuvent permettre d'identifier une personne parmi les passants se trouvant près de feux de signalisation. Ainsi, la question de savoir si une personne à laquelle se rapportent les informations est identifiée ou pas dépend des circonstances du cas d'espèce. »
>
> (G29, Avis 4/2007 sur le concept de données à caractère personnel, 20 juin 2007, WP 136, p. 14)

Contrairement à ce que le Gouvernement défend, la réponse à la question de savoir si une adresse IP peut ou non être une donnée personnelle n'emporte pas de réponse absolue et ne peut recevoir que des réponses circonstanciées. Afin de déterminer si les données transmises au serveur du ministère ont un caractère personnel en l'espèce, il convient donc de les examiner ensemble.

Lorsqu'est réalisée une opération de redirection d'une requête initiée par une personne physique avec un navigateur Web, de nombreuses données sont traitées.

Typiquement, les données concernées qui sont automatiquement transmises incluent :

- l'adresse IP ;
- des informations concernant le navigateur web utilisé, notamment la version précise du navigateur utilisé et celle du système d'exploitation, par exemple, le navigateur « Mozilla/5.0 (X11 ; Linux x86_64 ; rv :41.0) Gecko/20100101 Firefox/41.0 » ;
- la liste des fonctionnalités et des « plugins » activés sur le navigateur ;

– un ou plusieurs « cookies » comme, par exemple, des cookies d'authentification ou des cookies de session [4] ;
– l'adresse URL de la page qui a conduit à la requête [5], cette adresse pouvant elle-même comporter des informations très précises voire nominatives [6].

Ensemble, ces données permettent de créer une « empreinte » unique et propre à chaque individu, sans qu'il soit nécessaire d'effectuer un rapprochement avec les données détenues par les FAI, contrairement à ce que soutient le ministère. Cela a été démontré à de nombreuses reprises, y compris par des chercheurs de l'Institut national de recherche en informatique et en automatique (INRIA) [7]. Ces expériences établissent de manière incontestable que les traces laissées par les navigateurs permettent de créer une empreinte très détaillée, virtuellement unique, de l'utilisateur, et pas seulement de son ordinateur ou de son accès à Internet, et qu'il est en pratique illusoire de vouloir masquer cette empreinte.

Par conséquent, ces données acquièrent un caractère personnel permettant d'identifier un individu et leur communication par transmission constitue donc un traitement de données personnelles.

Au besoin, compte tenu de la technicité des questions ici abordées, le Conseil d'État pourra souhaiter procéder à une expertise au titre de l'article R. 621-1 du code de justice administrative pour éclairer son jugement sur cette question qui emporte de nombreuses conséquences, non seulement pour la présente affaire, mais aussi pour l'ensemble du droit des données personnelles et de la communication.

Ainsi qu'elles l'ont développé dans leur mémoire introductif, les associations requérantes appellent le Conseil d'État à tirer les conclusions qui s'imposent de l'existence d'un traitement de données personnelles induit par la consultation de la page d'information du ministère de l'intérieur : d'une part, il s'agit d'un traitement de données personnelles

4. Les cookies sont des blocs de données, assimilables à de très petits fichiers, qui sont utilisés pendant la navigation sur le Web pour conserver des informations entre deux pages ou entre deux visites. C'est par exemple l'information stockée dans un cookie, transmis par le navigateur à chaque clic, qui permet à certains sites Web d'identifier « tel utilisateur sur tel ordinateur » sans avoir à redemander son mot de passe. Ainsi par exemple le site sait qu'un cookie est associé à « Pierre, sur sa tablette » alors qu'un autre est associé à « Pierre, sur le Mac du travail ». Certains sites utilisent une notion connexe de *token* utilisés pour l'authentification, qui fonctionnent de manière très similaire.

Les cookies sont transmis au serveur dans la *requête*, bien avant qu'il soit possible pour le navigateur de savoir si le site est bien le site habituel, ou une autre page. Les cookies transmis sont tous ceux associés au nom de domaine du site, même s'il est l'objet d'une re-direction, ou si le nom de domaine a été racheté. Selon les techniques de développement utilisées par le site Web, les cookies peuvent contenir potentiellement n'importe quelle information, comme une adresse e-mail, un login, le nom en clair de l'utilisateur, ou un simple numéro d'identification chiffré.

5. Cette information, transmise systématiquement, est appelée le *Referer*, elle est utilisée pour savoir quelle page du Web fait référence à une autre page, par exemple pour établir des statistiques de navigation. C'est une des bases des mesures d'audience publicitaire, par exemple, ou de la mesure des contributions des apporteurs de trafic par les sites Web vivant de la publicité.

6. La page personnelle d'un utilisateur de Facebook, par exemple, comporte son nom d'utilisateur ou son numéro d'abonné, qui permet en un clic d'avoir son profil complet.

7. Voir en ce sens, cette étude scientifique publiée par l'INRIA :

Laperdrix et al., *Mitigating browser fingerprint tracking : multi-level reconfiguration and diversification.* 10th International Symposium on Software Engineering for Adaptive and Self-Managing Systems (SEAMS 2015), May 2015, Firenze, Italy, `https://hal.inria.fr/hal-01121108/document`

Ainsi que l'expérience de l'INRIA démontrant les empreintes laissées par le navigateur uniquement : *"Am I unique ?"* sur `https://amiunique.org/`

non prévu par un arrêté violant ainsi l'article 26, I, de la loi du 6 janvier 1978 et, d'autre part, la redirection implique l'existence d'une atteinte aux libertés non prévue par la loi contrairement à l'article 34 de la Constitution.

À ce dernier titre, les associations requérantes précisent que la consultation d'un site ne peut s'analyser comme un acte de communication public. Le fait de consulter un site et de lire son contenu est une activité qui relève de la sphère privée. La faculté pour le Gouvernement de savoir *via* des relevés d'adresses IP qu'une personne a utilisé son abonnement à Internet pour consulter un site revient à obtenir une liste des lecteurs d'un journal papier, ou d'intercepter les envois courrier de tels périodiques.

En tout état de cause, l'obtention de cette information par les services de l'État constitue à l'évidence une ingérence dans son droit à la vie privée, d'autant qu'elle est susceptible de servir à orienter l'action des services de police et de renseignement.

En effet, l'article 20 de la loi de programmation militaire ainsi que la loi n° 2015-912 du 24 juillet 2015 relative au renseignement permettent à plusieurs services du ministère de l'intérieur d'obtenir l'identité de l'abonné à partir de son adresse IP, sans que cette procédure d'accès ait à s'inscrire dans le cadre d'une procédure judiciaire. La même loi sur le renseignement va même plus loin en prévoyant que des dispositifs automatiques recevant ces informations (les « données de connexion ») en temps réel soient mis en place chez les fournisseurs d'accès (dispositif qui a été appelé « boîtes noires » lors des débats). C'est donc de mauvaise foi que le Gouvernement soutient que l'adresse IP de l'internaute ne lui permet pas d'en déterminer l'identité : cette information est disponible au même ministère que celui chargé de mettre en place le système informatique qui collecte illégalement ces informations, probablement dans les mêmes services.

II. LÉGALITÉ INTERNE

1. Inintelligibilité de la norme

À titre préliminaire, l'argument selon lequel le principe de confiance légitime aurait un champ d'application personnel limité aux opérateurs économiques est totalement infondé. Cela ne ressort en aucune mesure ni de la jurisprudence du Conseil d'État ni de la jurisprudence de la Cour de justice laquelle précise d'ailleurs que

> *« le principe de la protection de la confiance légitime est le corollaire du principe de sécurité juridique, qui exige que les règles de droit soient claires et précises, et vise à garantir la prévisibilité des situations et des relations juridiques relevant du droit communautaire*
> *(arrêt du 15 février 1996, Duff e.a., C-63/93, Rec. p. I-569, point 20). »* [1]

1.1. Sur la notion d'adresse électronique

Le Premier ministre défend que la notion d'adresse électronique employée dans le décret se borne à reprendre les termes de l'article 6-1 de la LCEN dont il fait application. Or, la notion d'adresse électronique étant centrale pour la mise en œuvre de la loi, il incombait au Gouvernement de préciser dans le décret cette notion, laquelle doit être tout à fait non-équivoque pour les personnes visées par l'application concrète du décret, à savoir notamment des fournisseurs d'accès à internet.

Les associations requérantes (dont deux sont fournisseurs d'accès à internet) critiquent le caractère imprécis et équivoque de la notion d'« adresse électronique » décrite dans le décret. En effet, la description ainsi faite ne permet pas de distinguer entre les nombreuses situations techniques différentes et emportant des niveaux d'ingérence inégaux dans les droits et libertés des utilisateurs de services de communication au public en ligne et de communications électroniques.

1. CJCE, arrêt du 18 mai 2000, Rombi, C-107/97, point 66

Dans son mémoire en réponse, le ministère de l'intérieur soutient que la notion d'adresse électronique décrite à l'article 2 du décret n° 2015-125 est suffisament claire et intelligible. Pour ce faire, il développe en quatre pages des explications techniques renvoyant à des documents non-normatifs [2] produits par l'AFNIC, ainsi qu'à une norme technique, la RFC 1034 [3].

Or, non seulement ces explications abondent dans le sens de l'argumentation développée par les requérantes, selon qui la norme n'est pas intelligible faute d'éléments précis et non-équivoques supplémentaires ; mais, en outre, les éléments supplémentaires apportés par le ministère dans ses réponses confirment le caractère ambigu et susceptible d'au moins deux significations de la notion d'adresse électronique.

En effet, dans un mémoire transmis le même jour, par le même ministère, signé de la même main, mais dans le cadre de l'affaire n° 389896, soit un recours contre le décret 2015-253, la notion d'adresse électronique est soutenue comme étant clairement définie par d'autres normes. En effet, dans ce second mémoire, le ministère renvoie vers la RFC 3986 [4].

En résumé, pour expliquer que les notions employées dans les décrets sont claires, le ministère fait référence à deux normes très différentes : l'une de 1987, l'autre de 2005. Si des développements si longs sont nécessaires pour arriver à une notion clairement intelligible, et si ces développements renvoient, pour les mêmes mots « *adresse électronique* » à deux notions aussi éloignées, c'est bien le signe évident que les notions sont mal exprimées dans les décrets [5].

Pour satisfaire à l'objectif de clarté et d'intelligibilité de la norme, le Gouvernement aurait pu, par exemple, dans le premier décret indiquer que « *les adresses électroniques sont des noms de domaines pleinement qualifiés (FQDN, au sens de la RFC 1034)* » et dans le second décret indiquer que « *les adresses électroniques sont des identifieurs de ressources uniformes (URI, au sens de la RFC 3986)* ».

En conclusion, les termes-mêmes choisis par le Gouvernement, et leur différence selon qu'il faut expliciter une notion mise en œuvre par le décret 2015-125 ou par le décret 2015-253, qui appliquent tous les deux le même article de la même loi, rendent manifeste le caractère inintelligible des notions d'adresse électronique employées dans le texte réglementaire.

---

2. Ces documents ne produisent pas de norme au sens juridique, bien entendu, mais ils n'en produisent pas non plus au sens technique. Ce ne sont pas des documents créant un protocole technique et indiquant son mode de fonctionnement, mais des documents pédagogiques, destinés au grand public, dont on ne peut pas attendre la même maîtrise technique que celle des ingénieurs spécialisés devant, eux, appliquer le dispositif attaqué.

3. Disponible en ligne sur le site web de l'IETF (Internet Engineering Task Force) à l'adresse `https://www.ietf.org/rfc/rfc1034.txt`, intitulée *Domain names – Concepts and Facilities*, de novembre 1987.

4. Disponible en ligne sur le site web de l'IETF à l'adresse `https://www.ietf.org/rfc/rfc3986.txt`, intitulé *Uniform Resource Identifier (URI) : Generic Syntax*, de janvier 2005.

5. Dans un domaine autre qu'Internet, on imagine mal un décret d'une telle portée s'appuyer sur une formulation technique aussi approximative : le terme « adresse électronique » tel qu'utilisé par les deux décrets cités (n° 2015-125 et n° 2015-253) est aussi imprécis que « pièce de moteur » pour l'industrie automobile, et correspond manifestement à deux notions très distantes (RFC 1034 et RFC 3986), qui sont plus précises, comme le seraient « filtre à air » et « bougie d'allumage », mais sans que rien dans le texte du décret puisse renvoyer à cette précision.

2. Atteinte disproportionnée à la liberté d'expression

Pour défendre le caractère proportionné de l'atteinte à la liberté d'expression, le Gouvernement soutient que la technique de redirection faite par un fournisseur d'accès internet consistant à « falsifier les réponses aux requêtes DNS en ne donnant pas l'adresse IP correspondant aux noms de domaine bloqués » (fin de page 14) est efficace et proportionnée.

Cependant, cette argumentation échoue à répondre aux motifs soulevés par les associations requérantes à l'encontre du décret. Le Gouvernement confond les **moyens techniques** du blocage (qui relèvent de la responsabilité des fournisseurs d'accès internet concernés) avec **la mesure d'injonction administrative** d'empêcher l'accès à une « liste noire » d'adresses électroniques.

En effet, le Gouvernement ne saurait imposer aux fournisseurs d'accès à Internet le moyen technique du blocage.

Premièrement, le décret ne prévoit pas cela. En effet, concernant les moyens techniques, le décret attaqué indique dans son article 3 :

> *« [...] 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 [...] »*

Par conséquent, le décret ne saurait imposer aux fournisseurs d'accès à Internet un moyen technique de blocage spécifique tel que celui consistant à falsifier les réponses aux requêtes DNS.

Deuxièmement, il ne pourrait en être autrement, sauf à porter atteinte à la liberté d'entreprise des fournisseurs d'accès à internet. En effet, suivant l'arrêt *Telekabel* de la Cour de Justice du 27 mars 2014 (affaire C-314/12), l'injonction d'empêcher l'accès au site doit laisser au fournisseur d'accès à internet :

> *« [...] le soin de déterminer les mesures concrètes à prendre pour atteindre le résultat visé de sorte que celui-ci peut choisir de mettre en place des mesures qui soient les mieux adaptées aux ressources et aux capacités dont il dispose et qui soient compatibles avec les autres obligations et défis auxquels il doit faire face dans l'exercice de son activité. » (point 52)*

Ainsi, le débat amené par les associations requérantes ne se borne pas à la critique de la mesure technique de blocage par falsifications de réponses du serveur DNS, mais au contraire les associations requérantes visent la nature disproportionnée et mal délimitée de la mesure d'injonction administrative d'empêcher l'accès à une liste noire d'adresses électroniques, notion aux contours arbitraires à défaut d'être techniquement intelligible pour les fournisseurs d'accès visés.

En effet, en vertu de l'article 2 du décret, les adresses électroniques sont décrites ainsi :

> *« [...] 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. »*

Compte-tenu des nombreuses implications rendues possibles en raison de la définition de cette notion d'adresse électronique, le décret autorise le Gouvernement à prendre

des mesures de blocage incompatibles avec la garantie des droits assurée par la Convention EDH.

En tout état de cause, plusieurs arguments avancés par le Premier ministre sont inopérants.

Sur le principe dit « de subsidiarité » de la LCEN

Les associations requérantes font valoir l'existence de mesures alternatives au blocage permettant d'atteindre les objectifs poursuivis par le législateur (voir la section 4.3.3 de la requête introductive d'instance).

En page 16, le Gouvernement écarte ce moyen en faisant valoir que le principe de subsidiarité « tel qu'il est défini à l'article 5 du traité sur l'Union européenne, est spécifique à l'ordre juridique de l'Union européenne et ne peut être utilement invoqué ».

Il n'aura pas échappé à tout lecteur de bonne foi de la requête introductive d'instance que les associations requérantes ne faisaient nullement référence au principe de subsidiarité dans l'ordre juridique de l'Union européenne. [6]

Le principe dont il s'agit est notamment prévu par la LCEN en matière de retrait de contenu illicite. Par exemple, l'article 6, I, 5 exige qu'une demande de retrait de contenu soit *d'abord* « adressée à l'auteur ou à l'éditeur des informations ou activités litigieuses » lorsqu'il est possible de les contacter, c'est *ensuite* seulement que la demande est adressée à l'hébergeur. *Enfin*, concernant l'autorité judiciaire, c'est « à défaut » de pouvoir préscrire une mesure à l'hébergeur, que le juge la prescrit *au fournisseur d'accès internet* (article 6, I, 8).

Ces demandes de retrait, adressées d'abord et directement à l'éditeur, sont plus respectueuses des droits et libertés. Passer outre ce processus de « subsidiarité » n'est pas justifié en l'espèce.

Sur les procédures judiciaires non transposables à une injonction administrative secrète

Le Gouvernement transpose à l'espèce les considérations de la Cour de Justice de l'Union européenne énoncées dans son arrêt *Telekabel* précité. Notamment, le Gouvernement avance que :

> « Il appartiendra, en réalité, comme l'a souligné la Cour, aux juridictions de première instance de vérifier, pour chaque mesure de blocage mise en œuvre dont elle serait saisie, que l'ingérence de l'autorité publique [...] se trouve justifiée [...]. C'est à l'occasion de cet examen, notamment que la réalité d'un sur-blocage et son impact pourront être mesurés. »

6. Le principe dit « de subsidiarité » en droit de services de communication en ligne est bien connu de la doctrine, ainsi que du législateur.

Voir par exemple le rapport d'information parlementaire sur la neutralité de l'internet et des réseaux, de Mesdames les députés Erhel et de La Raudière. Assemblée nationale, rapport n° 3336 du 13 avril 2011, disponible à l'adresse `http://www.assemblee-nationale.fr/13/rap-info/i3336.asp`

Voir également le rapport relatif à l'avis Net neutralité n° 2013-1 du 1er mars 2013 du Conseil national du numérique, disponible à l'adresse `http://www.cnnumerique.fr/wp-content/uploads/2013/03/130311-rapport-net-neutralite-VFINALE.pdf`

L'arrêt *Telekabel* concerne les injonctions **judiciaires** d'empêcher l'accès à des contenus contrefaisants. Or, en l'espèce, les injonctions critiquées sont d'ordre administratif et notamment, celles-ci ont un **caractère confidentiel** — la Cour de justice ne s'est pas prononcée sur ces aspects.

Par conséquent, cette motivation de la Cour ne saurait être transposée à ce litige.

Sur l'étude de l'OCLCTIC non communiquée

Le Gouvernement allègue que le blocage de nom de domaine implique un risque de sur-blocage minime, soit « 87% d'efficacité opérationnelle » (p. 14-15) selon une étude menée par l'OCLCTIC.

Force est de constater que cette étude n'a pas été versée aux débats et que les associations requérantes n'ont pas connaissance de son existance.

Ces éléments doivent donc être écartés des débats.

3. Absence de contrôle juridictionnel effectif

3.1. Sur l'absence de contrôle juridictionnel de la mesure de blocage

En l'espèce, il n'est pas constesté, premièrement, que la mesure en cause est motivée par une appréciation d'ordre pénal du contenu mis en cause – le Premier ministre le reconnaît d'ailleurs.

Deuxièmement, il n'est pas non plus contesté que la mesure de blocage constitue une restriction du droit à la liberté d'expression ainsi que de la liberté du public d'accéder aux informations publiées, tous deux garantis par l'article 10 de la Convention EDH.

Troisièmement, il n'est pas davantage contesté que la mesure de blocage intervient en dehors de toute procédure prévoyant effectivement aux éditeurs ou hébergeurs des contenus en cause la possibilité, préalablement à la mesure restrictive à leur égard, de pouvoir présenter leurs observations.

Quoiqu'il en soit, force est de constater que le Premier ministre n'apporte **aucune réponse** aux moyens tirés de **l'article 10 de la Conv. EDH** et de la jurisprudence de la Cour EDH, notamment l'arrêt du 17 juillet 2001, ***Association Ekin contre France*** (n° 39288/98) (cf. requête introductive d'instance, section 4.4.1. pages 34 et s.).

3.2. Sur l'ineffectivité du contrôle a posteriori ou du contrôle de la personnalité qualifiée

Le Premier ministre a également manqué de répondre aux moyens avancés par les associations requérantes au titre de l'article 6 de la Convention EDH, arguant que la mesure de blocage ne serait qu'une mesure de police administrative à l'encontre de laquelle l'article 6 de la Convention EDH ne pourrait être utilement invoqué.

Pour ce faire, il invoque une jurisprudence inapplicable au cas d'espèce. En effet, dans l'arrêt *SARL Le Madison* (n° 345903, 10 octobre 2012), le Conseil d'État exclut l'application de l'article 6 de la Convention au bénéfice des exploitants de débit de boissons dont la fermeture a été ordonnée par l'administration du seul fait d'infractions commis par des tiers, « indépendamment de toute responsabilité de l'exploitant ». *A contrario*, si la fermeture ainsi ordonnée avait été directement dépendante de l'engagement de la responsabilité de l'exploitant sur la base d'une accusation pénale, l'article 6 s'appliquerait. Or, en l'espèce, les mesures administratives dépendent directement de la qualification délictuelle des faits édités ou distribués. La qualification de ces délits ne saurait être faite « indépendamment de toute responsabilité » de leurs auteurs. Dès lors, une lecture *a contrario* de la jurisprudence citée offre à ces derniers le bénéfice de la Convention.

Le Premier Ministre développe une argumentation tout à fait contradictoire afin de prétendre que la mesure de blocage échappe à l'application de la Convention EDH et aux règles issues du procès équitable, il avance en effet que la mesure présenterait « un caractère exclusivement préventif ».

Cet argument est inopérant.

En effet, la Cour EDH définit largement une accusation en matière pénale comme le « reproche d'avoir accompli une infraction pénale », même lorsqu'il n'y a eu « en l'espèce ni arrestation ni inculpation » (CEDH, 27 février 1980, *Deweer c. Belgique*, n° 6903/75, points 43 et 46).

En l'espèce, en ordonnant le blocage, l'administration qualifie le service en cause comme étant constitutif des faits matériels des délits incriminés par les articles 227-23 et 421-2-5 du code pénal.

La mesure de blocage requise par l'administration auprès des fournisseurs d'accès internet est donc constitutive d'un « reproche d'avoir accompli une infraction pénale » et, dès lors, d'une accusation en matière pénale dirigée notamment contre l'éditeur du service bloqué.

Enfin, c'est en vain que, pour écarter cet argument, le Gouvernement prétend que, en droit français, « la mesure de blocage administratif de sites internet constitue une mesure de police », la Cour EDH considérant que les notions d'« "accusation en matière pénale" [et d']"accusé d'une infraction" [...] doivent s'entendre comme revêtant une portée "autonome" dans le contexte de la Convention, et non sur la base de leur sens en droit interne » (CEDH, 26 mars 1982, *Adolf c. Autriche*, § 30).

L'article 6, paragraphe 1, de la Convention EDH est donc bien applicable et l'éditeur est en droit de bénéficier des droits à un contrôle juridictionnel effectif (cf. requête introductive d'instance, section 4.4.2.).

Force est de constater que le Gouvernement ne conteste pas le caractère ineffectif des voies de recours ouvertes aux accusés en vertu de l'article 6 de la Convention EDH.

4. L'interception des correspondances privées

4.1. Exposé technique

Il ressort clairement du mémoire en défense présenté par le Gouvernement que celui-ci n'a pas perçu que le blocage d'un site Web par altération des réponses du DNS sur son nom emportait nécessairement des effets, variables d'un cas d'espèce à l'autre, sur les correspondances privées rattachées ou rattachables à ce nom de domaine. Il semble donc nécessaire de développer les explications techniques sur ce point.

Le système de DNS permet d'associer des informations, potentiellement de toutes natures, à des noms de domaines. L'approximation habituellement retenue pour les exposés de vulgarisation est de présenter le DNS comme un annuaire qui, à un nom de domaine donné (`edf.fr`, `www.fdn.fr` ou encore `www.somme.gouv.fr`) associe une adresse IP (`80.67.179.53`, associée au domaine `edgard.fdn.fr`). En réalité, le système permet d'associer à un nom plusieurs informations, chacune étant caractérisée par un type et une valeur.

Le type d'information le plus facilement compréhensible est le type `A`, qui permet de renseigner une adresse IPv4, ou le type `AAAA` qui permet de renseigner une adresse IPv6 [7].

Un autre type d'enregistrement associé fréquemment à un nom de domaine, mais moins connu du grand public, est le type `MX` (pour *Mail Exchanger*) qui indique le nom du système chargé de recevoir le courrier électronique à destination de ce domaine.

Ainsi, quand un courrier électronique est adressé à `bob@service.domaine.com`, la méthode [8] pour déterminer comment transporter ce courrier est la suivante (cf. RFC 974, *Mail routing and the domain system* [9]) :

1. Recherche sur le DNS d'un enregistrement de type `MX` associé à `service.domaine.com`.

   Si un tel enregistrement existe, il contient le nom de domaine d'un système informatique, recherche sur le DNS si un enregistrement de type `A` ou `AAAA` est associé à ce nom. Si oui, ce sytème sera utilisé pour transmettre le message.
2. À défaut, si aucun enregistrement de type `MX` n'est trouvé, recherche d'un enregistrement de type `A` ou de type `AAAA` associé à `service.domaine.com`. S'il en existe un, il est utilisé pour transmettre le message.
3. Si aucun enregistrement, ni de type `MX`, ni de type `A`, ni de type `AAAA` n'est trouvé, le message est considéré comme ne pouvant pas être délivré et l'expéditeur en est informé.

7. Le nom `AAAA` a été retenu parce que les adresses dans la version 6 du protocole IP sont quatre fois plus longues que dans la version 4. Par ailleurs leur représentation écrite est habituellement très différente, pour permettre des les écrire de manière dense et de les différencier immédiatement à première vue.

8. La méthode présentée ici, plus détaillée que ce qu'il est d'usage d'exposer pour de la vulgarisation, garde cependant dans l'ombre certains éléments de complexité : la capacité d'avoir plusieurs enregistrements de type `MX` pour un nom de domaine, les limitations liées à l'usage du *Canonical Name* pour la résolution en enregistrement de type `A` pour une valeur d'enregistrement `MX`, etc.

9. RFC 974, *Mail routing and the domain system*, janvier 1986, disponible en ligne sur le site Web de l'IETF `https://tools.ietf.org/html/rfc974`. Ce document est le plus ancien sur le mode de routage du courrier électronique par le nom de domaine. Le fonctionnement qu'il décrit a été amendé entre autres par les RFCs 1035, en 1987, 2821 en 2011 et 1912 en 1996.

Le moyen technique mis en avant dans la réponse du Premier ministre pour bloquer l'accès aux sites Web consiste à falsifier les réponses du système de DNS associées à un nom de domaine, en plaçant comme réponse un enregistrement de type `A` avec comme valeur l'adresse IPv4 d'un serveur géré par le ministère de l'intérieur.

Quel que soit le mode de configuration retenu par le nom de domaine avant l'action de blocage, la modification de cette configuration en altérant la réponse a des effets sur le transport des messages adressés à ce domaine. L'effet le plus fréquent est que ces messages seront présentés au serveur mis en place par le ministère de l'intérieur. Même si ce serveur refuse les messages, nous sommes bien en présence d'une correspondance privée dont l'acheminement a été intercepté, même s'il a été interrompu sans que le message soit délivré. Si, *contra legem*, le serveur du ministère de l'intérieur était configuré pour accepter ces messages [10], alors il y aurait bien interception et enregistrement d'une correspondance privée par un service de police, sans base légale.

Il peut également se présenter un certain nombre de cas où **des correspondances à destinations d'autres domaines** que celui visé par la décision soient interceptées, par exemple quand le serveur visé est un serveur de courrier électronique pour plusieurs domaines [11].

Le fait de falsifier la réponse à une requête de type `A` va nécessairement dérouter tout le trafic à destination de ce domaine, que ce soit le trafic direct (dont les trafic Web, mais pas seulement), ou le courrier électronique destiné à tout domaine qui utilisait cette adresse comme `MX`. Il convient de noter que ce cas de figure ne peut pas être détecté lors de la mise en place de la falsification : il n'existe aucun moyen de savoir si le nom de domaine visé par la demande de blocage est *utilisé* comme valeur d'un enregistrement `MX` d'un autre domaine, ou plus généralement s'il a d'autres usages que l'hébergement du site Web visé.

Par ailleurs, nous n'avons décrit ici que le système de transport et de routage des courriers électroniques. D'autres systèmes de messagerie existent, et tous reposent, à un moment ou à un autre, sur des enregistrements stockés dans le DNS. C'est le cas par exemple du protocole de messagerie instantannée XMPP (connu sous le nom de Jabber, et qui est à l'origine de Google Talk, par exemple). Leur mode de fonctionnement exact est plus complexe, parce qu'il est plus récent, et les risques d'interception par mégarde sont légèrement plus faibles. Leur fonctionnement sera, quoi qu'il en soit, altéré par une décision de blocage telle qu'elle est décrite dans le mémoire en défense du Gouvernement.

10. Par exemple à la suite d'une erreur du prestataire en charge de la gestion de ce serveur. Erreur relativement courante qui consiste à laisser, par défaut, un serveur informatique accepter tous les messages qu'on lui présente. Cette configuration est particulièrement courante, parce qu'elle évite, en cas d'erreur, qu'un message soit perdu.

11. Ainsi, une configuration de ce type là :
`domaine.com`, MX `www.domaine.com`
`mes-copains.com`, MX `www.domaine.com`
Si le domaine visé par la décision est `www.domaine.com` parce que la page Web `http://www.domaine.com/djihad` est déclarée illégale par l'OCLCTIC, alors toutes les correspondances à destination de `machin@domaine.com`, mais aussi de `truc@mes-copains.com` seront interceptées, le domaine `mes-copains.com` n'étant en rien partie à l'affaire.

4.2. Effets du décret attaqué

Le Gouvernement soutient, dans son mémoire en défense, comme les requérantes, qu'il n'est pas habilité à réaliser une interception de correspondance privée dans le contexte de ce décret.

En revanche, le Gouvernement se trompe quand il croit qu'un blocage par altération de la réponse des DNS permet de bloquer l'accès à un site Web sans avoir d'effet sur les correspondances privées rattachables au même nom de domaine, comme il vient d'être vu. Les requérantes rappellent que, dans la période où le ministère de l'intérieur préparait le décret attaqué, l'une d'entre elle, la Fédération FDN, a bénévolement et volontairement proposé d'apporter sa contribution sur ce sujet (une copie du courrier est jointe au présent mémoire), proposition à laquelle le ministère n'a jamais donné suite. L'objectif était, précisément, de s'assurer que quelques experts techniques issus de la société civile puissent vérifier que la méthode retenue par le ministère de l'intérieur ne crée pas trop de domages collatéraux.

Le fait que l'interception de correspondance privée soit un effet non désiré des mesures techniques décrites de manière approximative par le décret n'est pas en soi de nature à permettre au Premier ministre de déroger au respect du secret des correspondances.

Contrairement à ce que semble penser le Gouvernement, le fait que le blocage soit obtenu par l'altération des enregistrements renvoyés par le DNS n'apporte *aucune garantie* sur le fait que seul le service Web rattaché au nom de domaine serait touché par ce blocage, ni que ce seul service serait redirigé vers le serveur du ministère de l'intérieur.

Ce blocage d'un service de correspondance privée, ou l'interception de ces correspondances, selon le cas exact de configuration initiale du nom de domaine touché par la mesure, ne sont pas prévues par la loi. Partant, **cette disposition du décret est prise en excès de pouvoir**.

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

Le 24 octobre 2015, à Paris

Pour les associations requérantes,
Benjamin Bayart

Pièces produites : courrier de la Fédération FDN au ministère de l'intérieur pendant la préparation du décret, et réponse du ministère.