

Déclarations supplémentaires devant la Cour européenne des droits de l'homme dans les affaires FDN, FFDN et LQDN contre France — Annexe

1. Faits

1. Le 13 novembre 2014, le Parlement français a adopté la loi n° 2014-1353 renforçant les dispositions relatives à la lutte contre le terrorisme. L'article 12 de cette loi a ajouté à la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) l'article 6-1 (pièce n° 4) prévoyant que l'autorité administrative peut ordonner aux fournisseurs d'accès à Internet et « aux moteurs de recherche ou aux annuaires [sic] », respectivement, d'empêcher l'accès ou de cesser le référencement de listes d'adresses électroniques de services contrevenant aux articles 421-2-5 (pièce n° 3) et 227-23 (pièce n° 2) du code pénal réprimant la provocation ou l'apologie publique d'actes de terrorisme et réprimant la diffusion ou la représentation à caractère pornographique d'un mineur.
2. Les décrets n° 2015-125 (pièce n° 5 — blocage) et n° 2015-253 (pièce n° 6 — déréférencement) sont venus préciser les modalités d'application de l'article 6-1 de la LCEN. En particulier, le décret n° 2015-125 décrit les caractéristiques des « adresses électroniques » dont l'accès ou le référencement peuvent être empêchés sur notification de l'autorité administrative désignée (l'OCLCTIC). De plus, le décret n° 2015-125 prévoit une obligation pour les fournisseurs d'accès à Internet de mettre en place une redirection des adresses électroniques bloquées vers une page mise en ligne par le ministère de l'intérieur.
3. Les 31 mars et 29 avril 2015, trois associations – dont la présente – ont déposé devant le Conseil d'État français deux recours en excès de pouvoir demandant l'annulation de ces décrets organisant un filtrage (blocage ou déréférencement) de l'Internet (pièces n° 9 et 10). Elles contestaient alors la conformité de ces

décrets et des dispositions légales sur lesquelles ils se fondent, aux articles 6, 8 et 10 de la Convention EDH (la substance des moyens présentés par les association étant repris dans les présentes ou étant propres au droit français, ils ne seront pas détaillés ici).

4. Le 15 février 2016, le Conseil d'État a rejeté ces prétentions (pièce n° 11).
5. Pourtant, l'article 6-1 de la LCEN, avec ses décrets d'application, constitue une atteinte directe aux libertés de l'association requérante telles que reconnues par la Convention.
6. En effet, en premier lieu, afin de comprendre l'action de l'administration en matière de censure de l'information, l'association requérante a consulté de nombreux sites bloqués par l'administration. Ce faisant, elle a systématiquement été redirigée vers la page d'information hébergée par le ministère de l'intérieur, ce dernier ayant ainsi chaque fois été informé de ces accès, portant atteinte au respect de sa vie privée ainsi qu'à celui de ses adhérents ou salariés ayant contribué à cette entreprise.
7. En second lieu, l'association requérante est un fournisseur d'accès à Internet associatif qui sera directement amené à mettre en œuvre les techniques de blocage en cause et ainsi à porter atteinte aux libertés de ses membres — qu'elle représente.

2. Griefs ou exposé des violations

2.1. Violation de l'article 10

8. Pour être conforme à l'article 10 de la Conv. EDH, une restriction à la liberté d'expression (section 2.1.1), doit être prévue par la loi (section 2.1.2 page 4) et être nécessaire dans une société démocratique (section 2.1.3 page 6).

2.1.1. Restriction autorisée

9. **En droit**, une disposition conférant à l'administration de vastes prérogatives en matière d'interdiction de diffusion de publication s'analyse en soi en une

ingérence dans le droit à la liberté d'expression (Cour EDH, 17 juill. 2001, *Ekin c. France*, n° 39288/98, § 42).

10. D'une part, dans l'arrêt *Ekin c. France*, la Cour a décidé qu'une disposition conférant au ministre de l'intérieur français « de vastes prérogatives en matière d'interdiction administrative de diffusion de publications » étrangères (§ 58), notamment pour des contenus « de nature à causer des dangers pour l'ordre public » (§ 13), « s'analyse en soi en une « ingérence » dans le droit de la requérante à la liberté d'expression » (§ 42).
11. La Cour a analysé cette ingérence en visant *mutatis mutandis*, *Klass et autres c. Allemagne* § 41 (Cour EDH, Plén., 6 sept. 1978, *Klass c. All.*, n° 5029/71) en retenant que « 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 ».
12. D'autre part, suivant une jurisprudence constante de la Cour, la liberté d'expression inclut non seulement le droit de publier et d'éditer des contenus, mais elle inclut aussi le corollaire que constitue la liberté du public d'accéder aux informations publiées (voir notamment Cour EDH, 26 nov. 1991, *Observer c. R.-U.*, n° 13585/88, § 59).
13. Dès lors, une législation peut créer, par sa simple existence, la potentialité d'un filtrage entravant la liberté d'accéder à des informations publiées, qui s'analyse en soi en une ingérence à la liberté d'expression.
14. **En l'espèce**, l'article 6-1 de la LCEN et ses décrets d'application permettent à l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) d'exiger de tout fournisseur d'accès à Internet (FAI) et de tout exploitant de moteur de recherche ou d'annuaire d'empêcher l'accès à tout site Internet diffusant un contenu qu'il considère de son propre chef comme étant « l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique » ou

comme consistant à « provoquer directement à des actes de terrorisme ou de faire publiquement l’apologie de ces actes ».

15. **En conclusion**, la prérogative administrative de filtrage créée par l’article 6-1 de la LCEN, avec les risques d’arbitraire et d’abus qu’elle implique nécessairement, entrave la liberté d’expression — qu’il s’agisse de la liberté des personnes diffusant ou souhaitant diffuser des contenus licites ou de la liberté du public à recevoir des informations.

2.1.2. Prévues par la loi

16. **En droit**, l’article 10, paragraphe 2, de la convention prévoit que les restrictions à la liberté d’expression doivent être « prévues par la loi ». La Cour rappelle que les mots « prévue par la loi », au sens de l’article 10 § 2, « veulent d’abord que la mesure incriminée ait une base en droit interne, mais qu’ils ont trait aussi à la qualité de la loi en cause : ils exigent l’accessibilité de celle-ci à la personne concernée qui, de surcroît, doit pouvoir en prévoir les conséquences pour elle, et sa compatibilité avec la prééminence du droit » (Cour EDH, 17 juill. 2001, *Ekin c. France*, n° 39288/98, § 44).
17. La notion de loi doit être entendue dans son acception matérielle, elle inclut l’ensemble constitué par le droit écrit, y compris la jurisprudence qui l’interprète (voir, *mutatis mutandis*, Cour EDH, 24 avr. 1990, n° 11801/85, § 29).
18. La Cour a établi qu’« on ne peut considérer comme une ‘loi’ qu’une norme énoncée avec assez de précision pour permettre au citoyen de régler sa conduite ; en s’entourant au besoin de conseils éclairés, il doit être à même de prévoir, à un degré raisonnable dans les circonstances de la cause, les conséquences de nature à dériver d’un acte déterminé. » (Cour EDH, ch., 25 mars 1983, *Silver c. R-U*, n° 5947/72, §85)
19. À cet égard, dans l’arrêt *Ekin*, la Cour a précisé qu’il importait de savoir « si, au moment où l’arrêté ministériel du 29 avril 1988 fut pris, il existait une jurisprudence constante, claire et précise des juridictions françaises qui, venant

compléter la lettre de l'article 14 de la loi de 1881 modifiée, était de nature à permettre à la requérante de régler sa conduite en matière de publication d'ouvrages ».

20. **En l'espèce**, l'article 6-1 de la LCEN prévoit que les FAI et les exploiters de moteurs de recherche et d'annuaires doivent empêcher l'accès aux sites Internet accessibles aux « adresses électroniques » que leur notifie l'OCLCTIC.
21. Le décret n° 2015-125 (que vise le décret n° 2015-253) précise simplement que ces « adresses électroniques » doivent comporter un « nom de domaine », sans qu'il ne soit mentionné si ces adresses peuvent ou doivent comporter d'autres informations (tel que l'adresse d'une page Web précise – alors appelée « adresse URL » – ou bien le protocole sur lequel le blocage est demandé).
22. Ainsi, l'OCLCTIC est libre de décider arbitrairement de joindre ou non des informations complémentaires aux adresses dont il demande le filtrage (que ce soit par blocage ou par déréférencement. Or, en fonction de ces informations, les conséquences techniques du blocage sont extrêmement variées :
 1. s'il s'agit de bloquer globalement l'accès à un nom de domaine (par exemple, `monsite.fr`), tous les contenus, même licites, rattachés à ce nom de domaine seraient bloqués dans leur ensemble (par exemple, pour le site de YouTube, toutes les chaînes YouTube) ;
 2. s'il n'est pas précisé que le nom de domaine doit être bloqué sur un protocole précis (tel que le protocole Web) seront aussi bloquées toute « *communication électronique* » à destination du même nom de domaine, incluant les communications privées (par exemple, celles adressées à l'adresse `utilisateur@monsite.fr`) ;
 3. s'il s'agit de bloquer l'accès à l'adresse URL d'une page Web précise (par exemple `http://monsite.fr/articles/exemple.html`), les opérateurs devraient surveiller l'ensemble des communications électroniques susceptibles de correspondre à cette adresse pour pouvoir les bloquer, impliquant

d’analyser la totalité du trafic Internet et portant ainsi une atteinte significative au respect de la vie privée de l’ensemble des utilisateurs du réseau.

23. Ainsi, formulés de façon suffisamment vague pour permettre à l’OCLCTIC de définir arbitrairement l’étendue des mesures de filtrage qu’il ordonne, l’article 6-1 de la LCEN et ses décrets d’application ne sont pas accessibles aux personnes concernées — qu’il s’agisse des personnes diffusant un contenu ou un site censuré, du public dont l’accès à ces informations est empêché ou des personnes privées chargées de réaliser techniquement cette censure. Dès lors, ces personnes ne peuvent pas prévoir les conséquences concrètes de la loi en matière de liberté d’expression, ni ainsi régler leur conduite au regard de celles-ci.
24. Par ailleurs, il n’existe en France aucune jurisprudence « constante, claire et précise » qui, déterminant précisément la notion d’adresse électronique, soit « de nature à permettre [aux personnes concernées de régler [leur] conduite en matière de publication [en ligne] ». En effet, la seule juridiction ayant eu à interpréter cette notion a été le Conseil d’État qui, saisi par les requérantes de l’imprécision de celle-ci, s’est contenté de considérer que « les dispositions des décrets attaqués ne sont pas équivoques et sont suffisamment précises (§ 18) » (pièce n° 11), sans trancher d’aucune manière laquelle des différentes interprétations possibles devait en être retenue.
25. **En conclusion**, l’article 6-1 de la LCEN et ses décrets d’application autorisent une restriction qui n’est pas « prévue par la loi » et violent alors l’article 10, paragraphe 2, de la Convention.

2.1.3. Nécessaire dans une société démocratique

26. L’article 10, paragraphe 2, de la Convention exige que les restrictions faites à la liberté d’expression « constituent des mesures nécessaires, dans une société démocratique », à la poursuite d’objectifs légitimes. Telle qu’interprétée par la Cour, cette expression exige notamment que la restriction autorisée soit encadrée

de garanties contre les abus (section 2.1.3.1), apte à atteindre l'objectif poursuivi (section 2.1.3.2 page 9), ne constitue pas une restriction plus importante que celle nécessaire pour atteindre cet objectif (section 2.1.3.3 page 10) et que ce même objectif ne puisse pas être satisfait par des mesures moins restrictives (section 2.1.3.4 page 11).

2.1.3.1. Offrant des garanties contre les abus

27. **En droit**, dans l'arrêt *Ekin c. France* (Cour EDH, 17 juill. 2001, *Ekin c. France*, n° 39288/98), à propos de mesures de censure pouvant être prononcées par l'administration française, la Cour a décidé 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)

28. Ainsi, ne réunit pas des garanties suffisantes pour éviter les abus la mesure de censure que peut prononcer l'administration sans être précédée ni d'un contrôle juridictionnel ni de la possibilité pour la personne ayant diffusé l'information censurée de présenter ses observations.
29. **En l'espèce**, en premier lieu, l'article 6-1 de la LCEN et son décret d'application permettent à l'OCLCTIC – autorité administrative – d'obtenir des FAI la censure d'informations publiées sur Internet sans que cette mesure ne soit

soumise ni au contrôle ni à l'autorisation préalable d'aucune juridiction.

30. Cette situation, qui place la France dans une position singulière au sein du Conseil de l'Europe¹, a provoqué l'inquiétude du Secrétaire Général du Conseil de l'Europe, qui considère que « les autorités administratives qui ne sont pas suffisamment indépendantes de l'exécutif sont habilitées à ordonner le blocage de sites web. Cela entraîne parfois des restrictions sur des contenus internet qui ne tiennent pas dûment compte du principe de proportionnalité »². De même, cinq rapporteurs spéciaux du Haut-Commissariat des Nations Unies aux droits de l'homme ont aussi exprimé leurs « inquiétudes, notamment en ce qui concerne l'absence de contrôle judiciaire sur les procédures de blocage des sites internet »³.
31. En second lieu, l'OCLCTIC doit, avant de demander le blocage d'un site, chercher à obtenir le retrait du contenu litigieux qui est diffusé sur ce site auprès de l'éditeur ou de l'hébergeur de ce dernier. Toutefois, l'OCLCTIC n'est tenu de faire cette demande qu'auprès d'une seule de ces deux personnes : s'il la fait auprès de l'hébergeur, l'éditeur du site n'est aucunement informé de la mesure de retrait ou de blocage qu'il est susceptible de subir, ne pouvant présenter aucune observation à cet égard.
32. De plus, l'OCLCTIC n'est pas tenu de faire une demande de retrait préalable si ne figurent pas sur le site en cause les informations permettant d'en contacter l'éditeur ou l'hébergeur – et alors même que ces informations peuvent en principe

1. « Dans la plupart des États, ce sont les tribunaux qui conservent le pouvoir d'ordonner le retrait et le blocage d'un contenu. [...] Cependant, dans les pays tels que la France, la Russie et la Turquie, on trouve des autorités administratives avec un pouvoir considérable [...]. Elles peuvent avoir le droit dans certaines circonstances, d'ordonner à un intermédiaire technique de supprimer ou bloquer l'accès au contenu incriminé sans autorisation préalable d'un juge » (Institut suisse de droit comparé, 2015, *Étude comparative sur le blocage, le filtrage et le retrait de contenus illégaux sur Internet*, No. Avis 14-067, Lausanne, p. 780).

2. Communiqué de presse du Conseil de l'Europe, DC095(2016), *Le Secrétaire Général du Conseil de l'Europe préoccupé par la censure sur internet : les règles de blocage et de suppression de contenus illégaux doivent être transparentes et proportionnées*, 1er juin 2016.

3. Haut-Commissariat des Nations Unies aux droits de l'homme, *Déclaration publique sur la loi relative à l'état d'urgence et sur la loi relative à la surveillance des communications électroniques internationales*, 19 janvier 2016.

être très facilement réunies autrement. Dans ce cas, l'éditeur ne peut non plus présenter aucune observation, et l'hébergeur n'en est pas même prévenu.

33. **En conclusion**, l'article 6-1 de la LCEN ne réunit pas les garanties suffisantes pour éviter les abus en ce qu'il autorise l'administration à prendre des mesures de censures n'étant précédées ni d'un contrôle juridictionnel ni de la possibilité pour la personne ayant diffusé l'information censurée de présenter ses observations; l'ingérence ainsi permise ne peut dès lors être considérée comme nécessaire dans une société démocratique et violent donc l'article 10, paragraphe 2, de la Convention.
34. Cette conclusion est confortée par ce que, contrairement à l'espèce de l'arrêt *association Ekin contre France* – par ailleurs identique en tous points au cas présent –, les décisions de l'OCLCTIC ne font l'objet d'aucune mesure de publication de nature à porter à la connaissance du public l'existence de la mesure. Il faut souligner que ce manque est contraire aux recommandations du Comité des Ministres aux Etats membres du Conseil de l'Europe sur la liberté d'internet, qui prévoit que « l'Etat fournit au public, à temps et de manière appropriée, des informations sur les restrictions appliquées à la liberté de recevoir ou de communiquer des informations, expliquant quel site a été bloqué ou quelle information a été supprimée, notamment en précisant en détail le fondement juridique, la nécessité et la justification de telles restrictions, la décision de justice les autorisant et le droit de recours »⁴.

2.1.3.2. Apte à atteindre l'objectif poursuivi

35. En premier lieu, pour atteindre les objectifs poursuivis, la censure des contenus en cause doit pouvoir empêcher techniquement l'accès du public à ceux-ci. Si les textes d'application ne sont pas parfaitement explicites 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 le choix

4. Recommandation CM/Rec(2016)5 du Comité des Ministres aux Etats membres sur la liberté d'internet, point 2.2.5.

de l'administration française d'avoir recours à la technique de blocage par nom de domaine⁵. Or, cette technique est l'une des plus faciles à contourner – volontairement ou non – par l'utilisation d'outils courants liés à l'utilisation habituelle d'Internet, tels que 1) l'utilisation d'un serveur DNS différent de celui proposé par le fournisseur d'accès à Internet ; 2) l'utilisation de *Virtual Private Networks* ou VPN permettant d'accéder à Internet par un serveur situé à l'étranger ; 3) l'utilisation d'un outil comme Tor qui permet selon un récent rapport de l'assemblée parlementaire du Conseil de l'Europe de protéger sa vie privée sur Internet⁶ ou, enfin, 4) être abonné chez un FAI auquel n'ont pas été notifiées d'injonction administrative de blocage — ce qui est le cas d'une des associations requérantes.

36. En second lieu, les personnes ayant diffusé des contenus bloqués peuvent très facilement et très rapidement rendre ceux-ci de nouveaux accessibles au public français en faisant rediriger un nom de domaine n'ayant pas encore été visé par une mesure de blocage vers un site bloqué.
37. **En conclusion**, l'article 6-1 de la LCEN, ainsi que son décret d'application et sa mise en œuvre, ne permettent pas d'empêcher le public d'accéder aux contenus en cause, ne pouvant dès lors atteindre aucun des objectifs visés à l'article 10, paragraphe 2, de la Convention.

2.1.3.3. Limitée à ce qui est nécessaire

38. **En droit**, dans son arrêt *Yildirim* (Cour EDH, 2^e sect., 18 déc. 2012, *Yildirim c. Turquie*, n° 3111/10, § 68), la Cour a jugé que l'article 10, paragraphe 2, n'est pas respecté lorsque « le droit interne ne prévoit aucune garantie pour éviter qu'une mesure de blocage visant un site précis ne soit utilisée comme

5. Cette technique consiste pour les FAI à modifier le DNS qu'ils mettent à la disposition de leurs utilisateurs. Un DNS est un annuaire faisant la concordance entre une adresse IP et un nom de domaine, permettant aux utilisateurs de consulter un site Internet accessible à une adresse IP en ne connaissant que le nom de domaine associé à ce site. Ainsi, les FAI peuvent modifier leurs DNS pour qu'un nom de domaine ne soit plus associé à une adresse IP donnée. Le site accessible à cette adresse n'est alors plus accessible via ce nom de domaine.

6. OMTZIGT, Pieter, 26 janvier 2015. *Mass Surveillance*. Strasbourg, Assemblée parlementaire du Conseil de l'Europe, p. 13.

moyen de blocage général » – la mesure en cause dans cette affaire « consistait en un blocage général de tous les sites hébergés par Google Sites ». La Cour a ensuite précisé, dans son arrêt *Akdeniz* (Cour EDH, 2^e sect., 11 mars 2014, *Akdeniz c. Turq.*, n° 20877/10, § 28), que « 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 ».

39. **En l'espèce**, tel que déjà exposé, le mode de blocage retenu jusqu'à présent par l'administration consiste à demander le blocage d'une liste de noms de domaines. Or, 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, s'étendant par nature à tous les contenus diffusés sur le site accessible à ce nom de domaine.
40. **En conclusion**, les risques de sur-blocage étant particulièrement élevés s'agissant de la technique de blocage par nom de domaine, l'article 6-1 de la LCEN, ainsi que son décret d'application et sa mise en œuvre entraînent des restrictions à la liberté d'expression allant bien au delà de ce qui est nécessaire à la poursuite des objectifs qu'il serait légitime de poursuivre, et violent dès lors l'article 10, paragraphe 2, de la Convention.

2.1.3.4. Sans alternative moins restrictive

41. **En droit**, dans l'affaire *Yildirim* (Cour EDH, 2^e sect., 18 déc. 2012, *Yildirim c. Turquie*, n° 3111/10), la Cour a considéré comme contraire à l'article 10 de la Convention le fait pour la Turquie de « bloquer totalement l'accès à Google Sites » sans avoir « recherché si une mesure moins lourde pouvait être adoptée pour bloquer l'accès au site litigieux » (§64), « alors qu'une telle obligation découle directement de la Convention et de la jurisprudence de ses organes » (§ 66).
42. Telle obligation implique qu'une autorité souhaitant censurer un contenu sur Internet doit d'abord rechercher à obtenir le retrait de ce contenu sur le site où

il est diffusé avant de chercher à obtenir le blocage de ce site.

43. **En l'espèce**, en principe, l'article 6-1 de la LCEN prévoit que l'OCLCTIC doit d'abord formuler une demande de retrait du contenu en cause auprès de l'éditeur ou de l'hébergeur du site accueillant le contenu en question ; ces derniers disposent de 24 heures pour se conformer à cette demande ; à défaut, injonction est faite aux fournisseurs d'accès de bloquer l'accès au site.
44. Néanmoins, par exception, l'article 6-1, alinéa 2, de la LCEN dispose que ce principe ne s'applique plus si l'éditeur du site a omis d'y mentionné, tel qu'il y est tenu par l'article 6, III, de la LCEN,⁷ les informations permettant de le contacter lui ou son hébergeur. Dans ce dernier cas – très répandu en pratique, notamment s'agissant de sites non professionnels –, l'OCLCTIC peut alors directement demander aux FAI le blocage du contenu, sans devoir préalablement chercher à en obtenir le simple retrait.
45. Or, l'absence de telles informations sur le site n'empêche que dans de très rares cas l'OCLCTIC d'en contacter l'éditeur ou l'hébergeur. Ainsi, le site `islamic-news.info` (premier site que la presse française a identifié comme ayant été bloqué en application de ces dispositions) n'indiquait pas les mentions exigées par la loi mais les informations permettant d'en identifier l'hébergeur (OVH, une entreprise française) étaient facilement disponibles en ligne : une simple recherche auprès de l'hébergeur ou du vendeur du nom de domaine le permettant en principe.
46. **En conclusion**, l'article 6-1 permet à l'OCLCTIC d'exiger le blocage de sites sans avoir à rechercher d'obtenir préalablement le retrait des contenus en cause par tous les moyens les plus simples qu'il a à sa disposition, et viole donc

7. 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 précédentes les concernant.

l'article 10, paragraphe 2, de la Convention.

2.2. Violation de l'article 8

47. Le décret n° 2015-125 autorise une ingérence du ministère de l'intérieur dans l'exercice du droit au respect de la vie privée et de la correspondance de la population française (section 2.2.1) qui n'est ni prévue par la loi (section 2.2.2 page 15) ni nécessaire dans une société démocratique (section 2.2.3 page 15).

2.2.1. Ingérences autorisées

48. L'article 3, alinéa 4, du décret n° 2015-125 prévoit 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 ». En résulte une double ingérence : dans la vie privée (sectoin 2.2.1.1) et dans le secret des correspondances (section 2.2.1.2 page suivante).

2.2.1.1. Ingérence dans la vie privée

49. **En droit**, la Cour a jugé, dans son arrêt *Klass c. Allemagne* (Cour EDH, Plén., 6 sept. 1978, *Klass c. All.*, n° 5029/71, §41), que :

« 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. »

50. De même, elle a décidé, dans son arrêt *Amann c. Suisse* (Cour EDH, g^{de} ch., 16 févr. 2000, *Amann c. Suisse*, n° 27798/95, §68), que « la mémorisation par une autorité publique de données relatives à la vie privée d'un individu constitue une ingérence au sens de l'article 8. L'utilisation ultérieure des informations mémorisées importe peu. »

51. **En l'espèce**, lorsqu'une personne tente d'accéder à un site bloqué sur demande de l'OCLCTIC – sans avoir nécessairement conscience qu'il est bloqué ni qu'il diffuse des contenus dangereux –, sa connexion est redirigé vers une page d'information hébergée par le ministère de l'intérieur. De nombreuses données à caractère personnel la concernant sont alors automatiquement transmises au service du ministère hébergeant cette page (c'est une conséquence technique systématique de l'accès à la page).
52. Au nombre de ces données transmises figurent au moins l'adresse IP, des cookies et des informations sur les logiciels et terminaux utilisés. Ensemble, ces données permettent indéniablement au ministère d'identifier, directement ou indirectement, la totalité des personnes qui ont tenté d'accéder à un service bloqué. Il s'agirait d'une atteinte manifeste à la vie privée de ces personnes, dès lors que le ministère de l'intérieur se serait immiscé dans l'intimité des informations qu'elles consultent sur Internet.
53. De plus, il importe peu que, en pratique, ces personnes soient ou non identifiées : la possibilité technique que crée la loi suffit à placer les internautes dans la crainte d'être identifiés comme tels, altérant nécessairement leur comportement et les informations qu'ils sont enclins à consulter.

2.2.1.2. Ingérence dans le secret des correspondances

54. La redirection des internautes vers la page du ministère, tel qu'exposé plus tôt quand au blocage, se fait par nom de domaine. Ainsi, toute communication émise à destination du nom de domaine est redirigée vers le service du ministère de l'intérieur hébergeant la page d'information. Par exemple, si le service ayant pour nom de domaine `monsie.fr` était bloqué, un courrier électronique envoyé à l'adresse `martin@monsie.fr` serait automatiquement redirigé vers les services du ministère de l'intérieur, réalisant une interception de communication non prévue par la loi.

2.2.2. Prévues par la loi

55. Tel qu'exposé précédemment (section 2.1.2 page 4), les dispositions mettant en œuvre les mesures de blocage sont particulièrement imprécises et peu prévisibles, en violation de l'exigence de qualité de la loi imposée tant par l'article 10 que 8 de la Convention. Les dispositions en cause sont contraires à ce dernier article de ce seul fait.

2.2.3. Nécessaires dans une société démocratique

56. D'une part, l'information portée au public par la page d'information peut l'être de façon tout aussi efficace par une mesure ne portant aucune atteinte à la vie privée du public (section 2.2.3.1). D'autre part, la surveillance des personnes ayant consulté des services bloqués n'est pas encadrée des garanties minimales pour limiter les risques d'abus qu'elle crée (section 2.2.3.2 page suivante).

2.2.3.1. Mesure alternative pour informer le public

57. Le contenu de la page d'information pourrait être transmis aux FAI par le ministère de l'intérieur, leur enjoignant de l'afficher eux-même aux internautes tentant d'accéder à un site bloqué. La page d'information consultée serait donc hébergée par chaque FAI, et non par le ministère de l'intérieur. C'est d'ailleurs cette solution qui est actuellement mise en place en France par les FAI dans les cas de blocage de sites web suite à une décision de justice.
58. Ainsi, le public serait informé tout aussi efficacement du danger présenté par les contenus bloqués, mais personne ne pourrait savoir qui a tenté d'y accéder – les FAI ayant déjà par ailleurs en droit français l'interdiction de conserver les données permettant d'identifier les personnes qui consulteraient une telle page d'information, hébergée par eux.
59. En conclusion, la redirection du public vers une page d'information hébergée par les services du ministère de l'intérieur n'est pas nécessaire pour informer efficacement le public. Cette mesure ne saurait donc être considérée à cet égard comme « nécessaire, dans une société démocratique », violant l'article 8,

paragraphe 2, de la Convention.

2.2.3.2. Garanties encadrant la surveillance

60. **En droit**, dans son arrêt *Weber* (Cour EDH, 3^e sect., 29 juin 2006, *Weber c. All.*, n° 54934/00), la Cour a décidé que :

« Dans sa jurisprudence relative aux mesures de surveillance secrète, la Cour énonce les garanties minimales suivantes contre les abus de pouvoir que la loi doit renfermer : la nature des infractions susceptibles de donner lieu à un mandat d'interception, la définition des catégories de personnes susceptibles d'être mises sur écoute, la fixation d'une limite à la durée de l'exécution de la mesure, la procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies, les précautions à prendre pour la communication des données à d'autres parties, et les circonstances dans lesquelles peut ou doit s'opérer l'effacement ou la destruction des enregistrements. »

61. La Cour a ensuite eu l'occasion de préciser que ces exigences ne s'appliquaient pas aux seules mesures de surveillance secrète mais aussi à tous les « dispositifs de surveillance plus généraux » (Cour EDH, 4^e sect., 1 juill. 2008, *Liberty c. R-U*, n° 58243/00, § 63).
62. **En l'espèce**, le seul objectif qui pourrait être susceptible de justifier la redirection des internautes vers les services du ministère serait lié à l'identification des personnes tentant d'accéder aux contenus en cause. Or, la France a échoué à encadrer cette surveillance des garanties les plus simples permettant de limiter l'ingérence autorisée au stricte nécessaire.
63. En effet, ni la durée de conservation ni les conditions procédurales ou techniques d'exploitation des données ainsi collectées par les services du ministère de l'intérieur ne sont définies par le droit français.

64. **En conclusion**, la collecte par le ministère de l'intérieur de données permettant d'identifier les personnes ayant tenté d'accéder à un contenu bloqué pourrait être encadrée de garanties minimum qui limiterait l'ingérence permise. Cette mesure n'est ainsi pas « nécessaire, dans une société démocratique », pour atteindre un des objectifs limitatifs prévus à l'article 8, paragraphe 2, de la Convention, violant donc ce dernier.

2.3. Violation de l'article 6

65. **En droit**, en premier lieu, la Convention EDH, en son article 6, exige que toute personne accusée d'une infraction a droit à « être informé, dans le plus court délai, dans une langue qu'il comprend et d'une manière détaillée, de la nature et de la cause de l'accusation portée contre lui ».
66. En second lieu, au regard de l'exigence d'un procès équitable prévue par ce même article 6, la Cour a décidé, dans l'arrêt *Hentrich contre France* (Cour EDH, ch., 22 sept. 1994, *Hentrich c. France*, n° 13616/88, § 56), 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 » et que, dans l'espèce de cette affaire, ne respectait pas cette exigence la décision assortie d'une « motivation trop sommaire et générale pour permettre à Mme Hentrich de présenter une contestation raisonnée de » celle-ci.
67. Ainsi, pour ces deux raisons, une personne accusée d'une infraction doit être informée de la nature et de la cause de l'accusation portée contre elle et toute décision de l'autorité publique prise sur ce fondement doit être précisément motivée en droit et en fait.
68. **En l'espèce**, en premier lieu, l'article 2 du décret n° 2015-125 permet à l'OCLC-TIC de demander aux FAI le blocage « des services de communication au public en ligne contrevenant aux articles 227-23 et 421-2-5 du code pénal ». La mesure

de blocage ainsi ordonnée est donc constitutive d'une accusation en matière pénale formée par l'OCLCTIC contre l'éditeur du service bloqué, qualifiant ce service comme étant constitutif des faits incriminés par les dispositions pénales visées.

69. En second lieu, l'article 3 du même décret dispose que les FAI doivent garder secrète la liste des services que l'OCLCTIC leur a demandé de bloquer, sans exiger par ailleurs aucune forme de notification des mesures de blocage aux personnes concernées.
70. Certes, le décret prévoit que les internautes tentant d'accéder à un service bloqué doivent être redirigés par le FAI vers une page d'information leur indiquant que le service a été bloqué sur demande de l'administration. Néanmoins, cette redirection n'est effective que pour les personnes tentant d'accéder au service via le DNS d'un FAI destinataire de la demande de blocage : les personnes accédant à Internet via un FAI non destinataire de cette demande (que leur FAI soit étranger à la France ou simplement non visé par l'OCLCTIC), ainsi que celles utilisant un VPN ou un autre DNS que celui de leur FAI, n'ont pas l'occasion de consulter cette page d'information.
71. Au demeurant, cette page, destinée en priorité au public, ne comporte aucune précision factuelle détaillant les motifs du blocage – ne permettant pas même d'identifier le contenu précis qui, parmi la multitude de contenus pouvant être diffusés sur un site, a causé ce blocage.
72. Dès lors, les recours contentieux qui peuvent être envisagés par les personnes concernées contre cette décision ne peuvent être initiés que spontanément – sans en avoir été notifiées – et sans connaître les motifs précis qui ont conduit à l'adoption de cette décision – alors même que celle-ci constitue une accusation pénale. 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 de l'OCLCTIC.

73. **En conclusion**, en ne prévoyant aucune notification des personnes concernées par une mesure de blocage – et dès lors accusées d’avoir commis une infraction – ni de décision motivée de l’OCLCTIC pour prendre telle mesure, l’article 6-1 de la LCEN et son décret d’application violent l’article 6 de la Convention EDH.

3. Informations relatives à l’épuisement des voies de recours internes et au respect du délai fixé à l’article 35 § 1

74. Les 31 mars et 29 avril 2015, trois associations – dont la présente – ont déposé devant le Conseil d’État français deux recours en excès de pouvoir demandant l’annulation de ces décrets organisant un filtrage (blocage ou déréférencement) de l’Internet (pièces n° 9 et 10). Elles contestaient alors la conformité de ces décrets et des dispositions légales sur lesquelles ils se fondent, aux articles 6, 8 et 10 de la Convention EDH.
75. Le 15 février 2016, le Conseil d’État a rejeté ces prétentions (pièce n° 11), par une décision insusceptible de tous recours utiles en droit interne.