A/s : Observations des autorités françaises relatives à l'étude comparative sur le blocage, le filtrage et le retrait de contenus illégaux sur Internet dans les 47 Etats membres du Conseil de l'Europe. (08/04/2016)

I. Remarques préliminaires

Le cyberespace pose des difficultés pratiques et juridiques uniques dont le gouvernement français a pris pleinement conscience, notamment avec la loi n°2014-1353 du 13 novembre 2014.

Pour mémoire, il existe plusieurs modalités d'action contre le contenu dommageable d'un service de communication au public en ligne : retrait du contenu dommageable par l'hébergeur (ex : contenu offensant sur Facebook, Twitter, Youtube…) ; fermeture du site (ou assimilé tel un blog…) par l'hébergeur ; blocage d'accès à ce site proposant le contenu dommageable avec la coopération des fournisseurs d'accès Internet français et enfin mesure de déréférencement avec la coopération des moteurs de recherche Internet français.

Toutes ces techniques peuvent être complémentaires selon les cas de figure, et la mise en œuvre de ces mesures peut revenir à l'autorité administrative dans le cadre de la lutte contre la pédopornographie et l'apologie du terrorisme (art. 6-1 LCEN).

En dehors de ce champ d'application restreint, l'autorité judiciaire a le monopole d'intervention pour prévenir ou faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne (art. 6-I-8 LCEN). Une procédure spécifique de référé judiciaire a été également instituée en matière d'apologie du terrorisme sur saisine du ministère public (art. 706-23 CPP). Une procédure spécifique de référé est également prévue concernant les infractions de provocation à la commission de certaines infractions, à la discrimination, à la haine ou à la violence, à l'apologie de crime, et de contestation de crime contre l'humanité définies par les articles 24 et 24 bis de la loi du 29 juillet 1881 sur la liberté de la presse (article 50-1 de la même loi).

Si l'hébergeur est à l'étranger, les mesures de demandes de retrait peuvent se révéler inefficaces et les demandes de fermeture dépendantes des contraintes inhérentes à la procédure de coopération judiciaire internationale. Sur ce point, dans le cadre de l'Union européenne ainsi que de la Convention dite de Budapest (Conseil de l'Europe, mais également ratifiée par les Etats-Unis), la France est particulièrement active dans la recherche de solutions d'amélioration de ces coopérations.

Restent alors possibles les mesures de blocage par le fournisseur d'accès Internet français, notamment par voie de requête pouvant être rendue non contradictoirement (sous condition des articles 493 et 812 du code de procédure civile), et les mesures de déréférencement.

Si cette dernière option n'est pas expressément prévue par la LCEN au niveau judiciaire (au niveau administratif, voir le décret n° 2015-253 du 4 mars 2015), elle est désormais reconnue par une jurisprudence française récente (TGI de Paris, ordonnance de référé du 19 décembre 2014, Marie-France M./Google France et Google Inc), s'appuyant sur la jurisprudence de la Cour de Justice de l'Union Européenne (CJUE, 13 mai 2014 Google Spain SL, Google Inc. / (AEPD), Mario Costeja G.) qui consacre un droit pour tout ressortissant européen au déréférencement d'un contenu liée à sa vie privée, c'est-à-dire l'effacement des liens pointant vers des pages internet sur lesquelles son nom ou des informations le concernant sont présentes, sans pour autant que ces informations soient effacées du site source. **Ce point pourrait être ajouté au 3.2 du rapport de l'institut suisse de droit comparé (page 239).**

De manière générale, le suivi de l'effectivité de ces mesures est effectué à l'occasion des réunions du Groupe de contact permanent, présidé par le préfet chargé de la lutte contre les cybermenaces, auxquelles participent des représentants des sociétés de l'Internet ainsi que la mission de lutte contre la corruption et la cybercriminalité du ministère de la justice (direction des affaires criminelles et des grâces).

II. Observations sur les éléments de l'étude comparative concernant la France

- ***Au 2.2.1 " La protection de la sécurité nationale et des bonnes mœurs"***

L'expression « *bonnes mœurs* » utilisée notamment en page 225 n'est pas forcément pertinente en droit pénal, du fait de son caractère imprécis. Ainsi l'article 227-24 du code pénal qui réprime la fabrication, le transport et la diffusion de certains messages à des mineurs, comporte d'une liste limitative : « *message à caractère violent, incitant au terrorisme, pornographique ou de nature à porter gravement atteinte à la dignité humaine ou à inciter des mineurs à se livrer à des jeux les mettant physiquement en danger* ». De façon plus générale, l'autorité judiciaire est compétente selon la loi pour prescrire toutes mesures propres *« à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne* », ce point devant être apprécié au cas par cas. Si l'expression « *bonnes mœurs* » visait en réalité la « *pédopornographie* », il serait préférable de l'indiquer expressément.

En page 226, et afin d'éviter toute confusion, il convient de préciser que le mécanisme de l'article 706-23 du code de procédure pénale (cpp) ne s'applique que dans le cadre des actes terroristes, cet article figurant au « *Titre XV : de la poursuite, de l'instruction et du jugement des actes terroriste* » du cpp. Cette disposition est d'ailleurs citée à nouveau à la page 227, cette fois de manière claire mais sans mentionner la référence textuelle (article 706-23 cpp).

Au vu de ce qui est prévu par l'article 6-1 alinéa 1 de la loi pour la confiance dans l'économie numérique (LCEN), des imprécisions sont à signaler au second paragraphe de la page 232 rédigé comme suit : "En effet, en application de l'article 6-1 alinéa 1 LCEN, l'OCLCTIC ordonne aux fournisseurs d'hébergement sur internet des sites en cause et à leurs éditeurs de retirer ces contenus d'internet. Ce faisant, les fournisseurs d'hébergement et les éditeurs concernés sont tenus d'informer les fournisseurs d'accès. Si cette mesure n'est pas suivie par les hébergeurs et les éditeurs concernés, l'OCLCTIC pourra ordonner aux FAI de bloquer l'accès aux sites en cause".

Les autorités françaises proposent donc la reformulation suivante :

"En effet, en application de l'article 6-1 alinéa 1 de la LCEN, l'OCLCTIC **peut demander** aux fournisseurs d'hébergement sur internet des sites en cause **ou aux** éditeurs de retirer ces contenus d'internet. Ce faisant, **l'autorité administrative est tenue d'en informer simultanément** les fournisseurs d'accès. **En l'absence de retrait de ces contenus dans un délai de 24 heures**, l'OCLCTIC pourra **notifier** aux FAI **la liste des sites en cause qui devront alors empêcher sans délai l'accès à ces adresses**".

❖ *Au 4. "Surveillance générale d'internet"*

En page 240, les textes cités du Code de la sécurité intérieure (CSI) ne sont pas tous à jour de la loi n°2015-912 du 24 juillet 2015 relative au renseignement. En effet, l'article L246-1 CSI a été remplacé par l'article L851-1 CSI[1]. D'autre part, L241-2 CSI est certes encore en vigueur, mais de façon provisoire[2].

En page 241, concernant les « cyberpatrouilles », elles sont facilitées par une augmentation de moyens humains et matériels (par exemple le personnel de la plateforme PHAROS) et l'utilisation de l'enquête sous pseudonyme régie par l'article 706-87-1 du code de procédure pénale dans le cas d'atteinte en bande organisée aux Systèmes de traitement automatisé de données (STAD) mis en œuvre par l'Etat (art. 323-4-1 du code pénal).

❖ *Au 5. "Évaluation au regard de la jurisprudence de la Cour européenne des droits de l'homme"*

Les autorités françaises précisent que le Conseil d'Etat, par une décision du 15 février 2016 (CE, Association French Dat Network et autres, décision n°389140), a rejeté les recours pour excès de pouvoir déposés par les associations French Data Network, La Quadrature du Net et la Fédération des fournisseurs d'accès à internet associatifs contre le décret 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 pornographiques et contre le décret du 4 mars 2015 relatif au déréférencement des mêmes sites, pris pour l'application de l'article 6-1 de la loi pour la confiance dans l'économie numérique.

---

[1] ***« Article L851-1*** *(remplace L246-1 CSI, p240), créé par LOI n°2015-912 du 24 juillet 2015 - art. 5*

Dans les conditions prévues au chapitre Ier du titre II du présent livre, peut être autorisé le recueil, auprès des opérateurs de communications électroniques et des personnes mentionnées à l'article L. 34-1 du code des postes et des communications électroniques ainsi que des personnes mentionnées aux 1 et 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, des informations ou documents traités ou conservés par leurs réseaux ou services de communications électroniques, y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications.
Par dérogation à l'article L. 821-2, les demandes écrites et motivées portant sur les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, ou au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée sont directement transmises à la Commission nationale de contrôle des techniques de renseignement par les agents individuellement désignés et habilités des services de renseignement mentionnés aux articles L. 811-2 et L. 811-4. La commission rend son avis dans les conditions prévues àl'article L. 821-3.
Un service du Premier ministre est chargé de recueillir les informations ou documents auprès des opérateurs et des personnes mentionnés au premier alinéa du présent article. La Commission nationale de contrôle des techniques de renseignement dispose d'un accès permanent, complet, direct et immédiat aux informations ou documents collectés.
Les modalités d'application du présent article sont fixées par décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés et de la Commission nationale de contrôle des techniques de renseignement.

[2] *En application du III de l'article 26 de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement, le présent article, abrogé par le I de l'article 23 de la même loi, demeure applicable aux services relevant du ministre de la défense, du ministre de l'intérieur ou des ministres chargés de l'économie, du budget ou des douanes, autres que ceux mentionnés aux articles L. 811-2 et R. 811-1 du code de la sécurité intérieure, jusqu'à l'entrée en vigueur du décret prévu à l'article L. 811-4 du même code. Jusqu'à cette date, la Commission nationale de contrôle des techniques de renseignement exerce les compétences confiées par le présent titre à la Commission nationale de contrôle des interceptions de sécurité. »*

Dans cette décision, le Conseil d'Etat a considéré que **les restrictions apportées à la liberté d'expression par ces deux décrets étaient prévues par la loi, répondaient à des finalités légitimes et étaient adaptées, nécessaires et proportionnées à l'objectif poursuivi et ne constituaient pas une atteinte disproportionnée à la liberté d'expression garantie par l'article 10 de la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales** (cf. observations sur les conclusions provisoires *infra*).

- ***Sur les conclusions provisoires***

Les conclusions provisoires de l'étude conduite par l'Institut suisse de droit comparé sont les suivantes :

« En conclusion, la compatibilité du dispositif de blocage administratif des sites internet incitant à commettre des actes terroristes ou en faisant l'apologie avec la jurisprudence naissante de la Cour européenne des droits de l'homme en la matière n'est pas acquise. D'une part, si la possibilité de restreindre la liberté d'expression sans intervention préalable d'un juge semble acquise pour le Conseil Constitutionnel dans le cadre de sites internet qui «diffusent des images de pornographie infantile», il n'en reste pas moins que ce blocage sur ordre administratif repose sur un constat objectif, c'est-à-dire la présence d'images de pornographie impliquant des enfants. La qualification des notions de provocation à des actes terroriste et d'apologie du terrorisme peut toutefois s'avérer nettement plus délicate en ce qu'elle constitue un sujet beaucoup plus subjectif. D'autre part, l'interprétation des notions de provocation à d'actes terroristes ou d'apologie au terrorisme est réalisée sur la base de règles de droit et sous le double contrôle de la personnalité qualifiée au sein de la CNIL d'abord et du juge ensuite dans le cadre d'un recours judiciaire contre la décision administrative de blocage ou retrait.

Enfin, en ce qui concerne la lutte contre les discours de haine sur Internet, il convient de mentionner l'Avis de la Commission nationale consultative des droits de l'homme qui a été adopté le 12 Février 2015. Dans cet avis, la CNCDH fait plusieurs recommandations, parmi lesquelles l'amendement de la LCEN en vue d'identifier les intermédiaires de l'Internet qui jouent un «rôle actif» et d'imposer à ces intermédiaires une obligation de détecter de manière proactive le contenu considéré comme du discours de haine ainsi que l'obligation d'informer les autorités compétentes de l'existence de ce contenu. La CNCDH propose également la création d'une autorité administrative indépendante spécifique chargée notamment d'accompagner les hébergeurs et des fournisseurs d'accès à Internet dans leur tâche d'identification des discours de haine sur internet. »

Ces deux questions vont être examinées successivement :

- **Compatibilité du dispositif de blocage administratif français avec la jurisprudence de la Cour européenne des droits de l'Homme**

A ce sujet, les considérants 11 à 16 de l'**avis de compatibilité rendu par le Conseil d'Etat français** (décision n°389140 du 15 février 2016) sont reproduits ci-dessous :

« 11. Considérant qu'aux termes de l'article 10 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales : " 1. 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. / 2. 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 " ; qu'il résulte de ces stipulations que les restrictions apportées à la liberté d'expression ne peuvent être autorisées que si elles sont prévues par la loi, répondent à des finalités légitimes et sont adaptées, nécessaires et proportionnées à l'objectif poursuivi ;

12. Considérant, en premier lieu, que les dispositifs de blocage et de déréférencement prévus par les décrets attaqués ont pour objectifs légitimes, d'une part, de restreindre, pour les internautes de bonne foi, l'accès aux sites provoquant à des actes de terrorisme ou en faisant l'apologie et aux sites diffusant des images et représentations de mineurs à caractère pornographique et, d'autre part, de gêner l'accès volontaire de certains internautes à ces contenus ;

13. Considérant, en deuxième lieu, qu'au regard de ces objectifs, la circonstance qu'il serait techniquement possible, pour certains, de contourner le blocage ou le déréférencement des sites au contenu illégal ne peut conduire à regarder ces dispositifs comme inadaptés aux objectifs poursuivis ;

14. Considérant, en troisième lieu, **qu'il ne résulte pas des stipulations précitées de l'article 10 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales que les mesures de blocage et de déréférencement en cause ne puissent être ordonnées que par un juge** ;

15. Considérant, en quatrième lieu, que les risques limités de " sur-blocage " résultant de la technique du blocage par nom de domaine ne sauraient conduire à regarder comme disproportionné le dispositif de blocage prévu par l'article 6-1 de la loi du 21 juin 2004 ; qu'il ne ressort pas des pièces du dossier que d'autres dispositifs, impliquant une ingérence dans l'exercice des droits des individus moins forte, permettraient d'atteindre les objectifs poursuivis ;

16. Considérant, en cinquième lieu, que le troisième alinéa de l'article 6-1 de la loi du 21 juin 2004 prévoit la transmission de la liste des adresses électroniques à bloquer ou à déréférencer à une personnalité qualifiée, désignée en son sein par la Commission nationale de l'informatique et des libertés, qui " s'assure de la régularité et des conditions d'établissement, de mise à jour, de communication et d'utilisation de la liste ", peut émettre des recommandations à l'autorité administrative et, le cas échéant, saisir le juge administratif ; que les articles 5 des décrets attaqués prévoient que cette personnalité qualifiée " dispose pour l'exercice de ses fonctions des services de la Commission nationale de l'informatique et des libertés ", peut bénéficier de l'assistance d'un interprète et se voit transmettre les motifs des demandes de retrait adressés aux éditeurs et aux hébergeurs ; qu'elle dispose ainsi des moyens humains, techniques et financiers nécessaires pour s'assurer de la régularité des demandes de blocage et de déréférencement formulées par l'autorité administrative ; que la décision de cette dernière est par ailleurs susceptible d'être contestée à tout moment et par toute personne intéressée devant le juge administratif, le cas échéant en référé ; qu'enfin, les articles 4 des décrets attaqués prévoient que " l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication vérifie au moins chaque trimestre que les adresses électroniques notifiées ont toujours un contenu présentant un caractère illicite " et que, si tel n'est plus le cas, ces adresses sont retirées de la liste et les mesures de blocage et de déréférencement levées ; que, contrairement à ce qui est soutenu, ces différents éléments sont de nature à permettre une mise en oeuvre des dispositifs de blocage et de déréférencement contestés sans atteinte disproportionnée à la liberté d'expression. »

A noter également que la validité du décret du 4 mars 2015 relatif au déréférencement est affirmée dans le considérant 8 : « *le décret […] ne prévoit ainsi aucune restriction à la liberté de communication qui ne résulte déjà de la loi ; que le moyen tiré de ce qu'il serait entaché d'incompétence sur ce point doit donc être écarté* ».

Afin d'être complet, il convient d'évoquer les dispositions de blocage administratif telles que prévues à l'article 11 II de la loi du 3 avril 1955 relative à l'Etat d'urgence, modifiée par la loi n°2015-1501 du 20 novembre 2015. A notre connaissance, elles n'ont pas fait l'objet d'une question prioritaire de constitutionnalité (QPC)[3].

Pour mémoire, la disposition prévue dans le cadre de l'état d'urgence est la suivante :

« II. - Le ministre de l'intérieur peut prendre toute mesure pour assurer l'interruption de tout service de communication au public en ligne provoquant à la commission d'actes de terrorisme ou en faisant l'apologie. »

Les pouvoirs de l'administration sont ici accrus dans la mesure où celle-ci n'a plus besoin de formuler une demande de retrait préalable des contenus concernés ni à saisir la « personne qualifiée » désignée par la CNIL.

Toutefois, toute personne intéressée par le blocage ou le retrait du site pourra, a posteriori, exercer un recours administratif devant le ministre de l'Intérieur lui-même, ou contester l'abus supposé devant le juge administratif.

Si la jurisprudence de la Cour européenne des droits de l'Homme a rappelé que la liberté d'expression protège *« non seulement les informations ou idées accueillies avec faveur ou considérées comme inoffensives ou indifférentes, mais aussi celles qui heurtent, choquent ou inquiètent* »[4], et doit ainsi permettre l'expression sur Internet de profonds désaccord avec la politique extérieure de la France, elle ne peut couvrir des contenus relatifs à l'apologie du terrorisme ou provoquant à des actes de terrorisme, ces faits étant pénalement sanctionnable[5].

La définition de l'apologie, en tant que « *discours ou écrit glorifiant un acte expressément réprimé par la loi pénale* » (Dictionnaire Larousse), est suffisamment explicite pour préserver la liberté d'expression et ainsi éviter la censure sur Internet de critiques visant la politique française, sa diplomatie ou ses choix militaires.

- **Concernant un éventuel renforcement du dispositif de lutte contre le discours de haine sur Internet**

Il paraît délicat d'imposer une obligation générale de surveillance visant ce type de contenu aux acteurs de l'Internet, en termes de faisabilité technique et de proportionnalité. En réalité, leur coopération dans le dispositif actuel et leur réactivité dans le cadre des procédures internes de signalement de contenu « offensant » semble suffisantes en l'état.

[3] A l'inverse de l'article 11 I concernant les saisies de matériel informatique dans le cadre des perquisitions adminstratives (décision n°2016-536 QPC du conseil constitutionnel).
[4] Arrêt Association Ekin c/ France du 17 juillet 2001.
[5] Article 421-5 du code pénal, peine de 7 ans et de 100 000 euros d'amendes lorsque les faits sont commis en utilisant un service de communication au public en ligne

Comme précédemment évoqué, les acteurs de l'Internet doivent de manière régulière faire état des progrès significatifs dans cette coopération à l'occasion des réunions du Groupe de contact permanant, sous la présidence du préfet délégué à la lutte contre les cybermenaces.

La création d'une nouvelle autorité administrative indépendante chargée d'accompagner les hébergeurs et fournisseur d'accès à Internet dans leur tâche d'identification des discours de haine sur Internet est dès lors superflue, d'autant que les personnes qualifiées désignées par la CNIL vérifiant l'adéquation des contenus filtrés, bloquées, retirés, déréférencés remplissent déjà a posteriori ce rôle auprès de l'OCLCTIC en charge de la plateforme PHAROS.