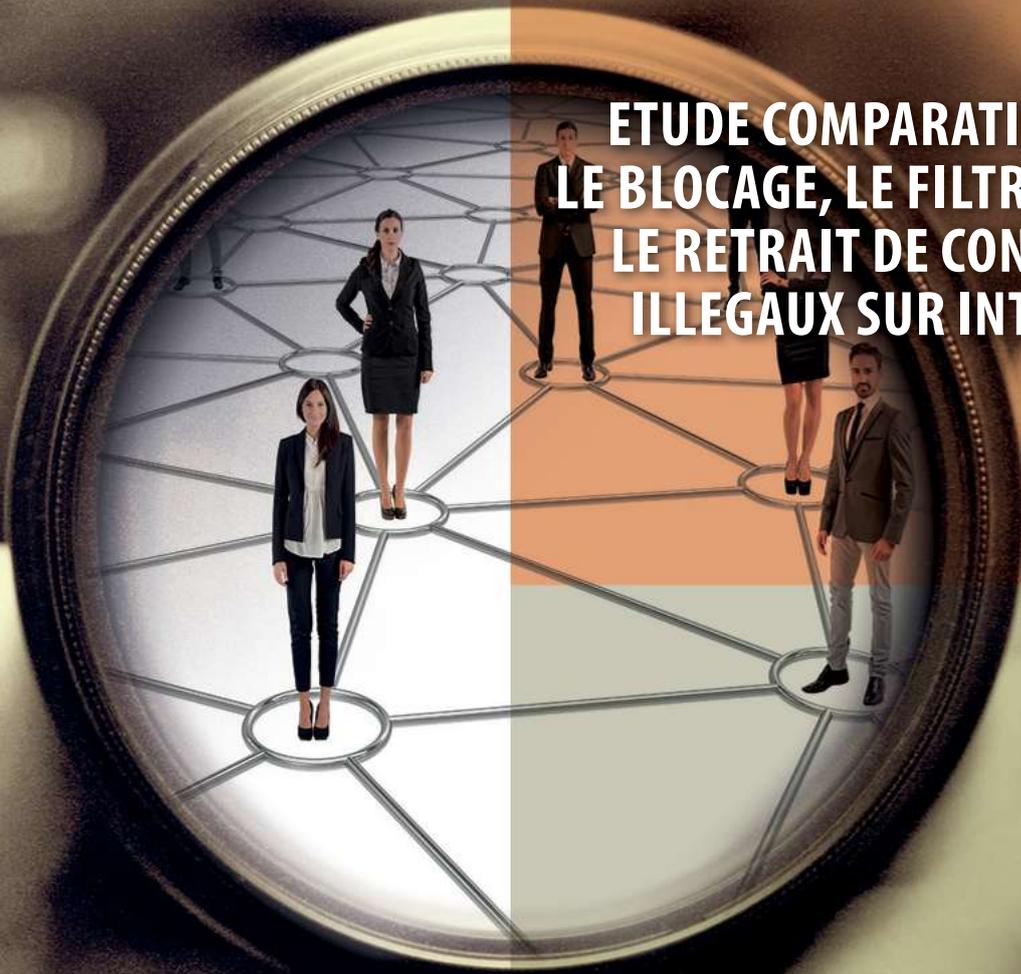


**ETUDE COMPARATIVE SUR
LE BLOCAGE, LE FILTRAGE ET
LE RETRAIT DE CONTENUS
ILLEGAUX SUR INTERNET**



www.coe.int/freedomofexpression

ÉTUDE COMPARATIVE SUR LE BLOCAGE, LE FILTRAGE ET LE RETRAIT DE CONTENUS ILLÉGAUX SUR INTERNET

Ce document fait partie de l'Étude comparative sur le blocage, le filtrage et le retrait de contenus illégaux sur internet dans les 47 États membres du Conseil de l'Europe, qui a été préparée par l'Institut suisse de droit comparé à l'invitation du Secrétaire Général. Les opinions exprimées dans ce document n'engagent pas la responsabilité du Conseil de l'Europe. Elles ne donnent, des instruments juridiques qu'il mentionne, aucune interprétation officielle pouvant lier les gouvernements des États membres du Conseil de l'Europe, les organes statutaires du Conseil de l'Europe ou la Cour européenne des droits de l'homme.

Lausanne, 20 décembre 2015

Conseil de l'Europe

Édition anglaise :

*Comparative study on blocking, filtering and
take-down of illegal internet content*

Toute demande de reproduction ou de traduction de tout ou d'une partie de ce document doit être adressée à la Direction de la communication (F-67075 Strasbourg ou publishing@coe.int). Toute autre correspondance relative à ce document doit être adressée à la Direction Générale Droits de l'Homme et État de droit.

Couverture et mise en pages :
Service de la production des documents et des publications (SPDP) Conseil de l'Europe

© Conseil de l'Europe, février 2017

Imprimé dans les ateliers
du Conseil de l'Europe.

RÉSUMÉ

MODÈLES RÉGLEMENTAIRES

Dans les différents États examinés, le blocage et le retrait de contenus en ligne sont souvent traités de façon similaire, et, dans les pays disposant d'un cadre législatif ciblé, ils sont souvent règlementés par le même ensemble de règles. On distingue deux catégories générales de « modèle » réglementaire.

Premièrement, il y a les **pays dépourvus de législation spécifique** sur la question du blocage, filtrage et retrait des contenus illégaux sur internet: ces États ne se sont pas dotés d'un régime législatif ou réglementaire définissant les conditions et les procédures à respecter par ceux qui pratiquent le blocage, le filtrage ou le retrait de contenus en ligne. Un des arguments souvent avancés dans ce contexte est l'impossibilité pour le législateur de suivre le rythme des évolutions technologiques. Cependant, la raison sous-jacente à l'absence d'un cadre législatif peut également se trouver dans la tradition juridique du pays concerné.

En l'absence d'un cadre juridique spécifique ou ciblé, **plusieurs pays s'appuient sur un cadre juridique « général » – c'est-à-dire qui n'est pas spécifique à l'internet – existant** pour mettre en œuvre – ce qui constitue en général – un blocage ou retrait limité de contenus illégaux en ligne. C'est notamment le cas en Allemagne, en Autriche, aux Pays-Bas, au Royaume-Uni, en Irlande, en Pologne, en République tchèque et en Suisse. Ces pays étant de plus en plus confrontés à la réalité des différends relatifs à des contenus internet, l'absence d'intervention du législateur s'y est avérée être problématique. Ces dernières années, différents mécanismes ont été employés pour pallier le vide réglementaire et pour résoudre des problèmes particuliers. Certaines juridictions ont même choisi de combiner des approches différentes, autrement dit de maintenir un cadre en grande partie non règlementé tout en intervenant sur le plan législatif ou politique dans des domaines spécifiques. De même, dans certaines juridictions, **le secteur privé a adopté une autoréglementation** pour combler le vide laissé par le choix du législateur de ne pas intervenir dans le domaine en question. D'autres pays s'en remettent aux **tribunaux municipaux** pour préserver, autant que possible, le nécessaire équilibre entre liberté d'expression, d'une part, et sûreté d'internet et protection d'autres droits fondamentaux, d'autre part.

Deuxièmement, dans de nombreuses juridictions, le législateur est intervenu afin de mettre en place un **cadre juridique visant à règlementer internet et d'autres médias numériques**, y compris le blocage, le filtrage et la suppression de contenus en ligne. Un tel régime législatif définit généralement les fondements juridiques du blocage ou de la suppression, l'autorité administrative ou judiciaire habilitée à prendre les mesures pertinentes et les procédures à suivre.

Alors que les **motifs les plus courants d'adoption de mesures de blocage, filtrage ou retrait** sont définis de manière exhaustive et explicite dans la législation de la plupart des pays qui optent pour ce modèle réglementaire, certaines juridictions ont, dans les faits, étendu le champ des motifs pour lesquels une décision de blocage ou de suppression peut être légitimement prise – souvent par une modification de la législation ou une interprétation créative par l'autorité judiciaire.

Procédure

En ce qui concerne **le matériel illicite touchant à la pédopornographie, au terrorisme, à la criminalité (en particulier, les crimes haineux) et à la sécurité nationale**, bon nombre d'États disposant de règles juridiques

ciblées sur le retrait de contenus en ligne prévoient le blocage urgent de ce type contenu sans qu'une décision de justice à cet effet ne soit nécessaire. Les autorités administratives, autorités policières ou procureurs disposent de pouvoirs spécifiques pour imposer aux fournisseurs d'accès à l'internet de bloquer l'accès sans décision judiciaire préalable. Il est courant que, sans en informer le fournisseur de contenu ou l'hébergeur, de telles ordonnances imposent au fournisseur d'accès à l'internet d'appliquer des mesures dans un délai de 24 heures. Dans d'autres pays, tels que la Finlande où une décision judiciaire est requise, les fournisseurs d'hébergement ayant connaissance des contenus en question devraient les éliminer sur une base volontaire sans décision judiciaire et le notifier au fournisseur de contenu, ce qui permet à ce dernier de contester la mesure devant la justice.

Un certain nombre de régimes nationaux imposent à l'autorité administrative compétente d'**obtenir après coup l'agrément de sa décision par le tribunal compétent**, tandis que d'autres régimes imposent de mettre, à l'adresse du matériel bloqué, une **page d'information** expliquant pourquoi le matériel est bloqué et comment la décision peut être contestée. Dans la plupart des pays, les parties intéressées ont la **possibilité de contester** les mesures de blocage sur la base des dispositions de procédure pénale (ou le cas échéant, civile) usuelles.

En particulier, s'agissant du matériel touchant à la pédopornographie et à d'autres crimes graves, de nombreux pays adoptent un **système de « liste »** dans le cadre duquel l'autorité administrative compétente tient et actualise une liste centrale d'URL ou de noms de domaine bloqués. Cette liste est notifiée aux fournisseurs d'accès à internet concernés qui sont tenus de veiller à l'effectivité du blocage.

Dans de nombreux États, le retrait et le blocage de matériel qui **porte atteinte aux droits relatifs à la propriété intellectuelle** et à la vie privée ou à la diffamation sont effectués ou autorisés **en vertu d'une décision judiciaire exclusivement**. Certains pays ont introduit des procédures substitutives de notification et de retrait pour contourner la nécessité d'une action en justice. Dans certains pays, il existe une procédure permettant aux personnes qui ont des droits à cet égard d'obtenir la suppression de matériel prétendument illégal, à condition que le fournisseur de contenu concerné ait droit à une procédure régulière pour contester la suppression. En ce qui concerne en particulier le **matériel diffamatoire ou d'autres contenus qui portent atteinte au droit au respect de la vie privée**, l'application de mesures aux fins de laquelle **de nombreux pays ont prévu une procédure de « notification et retrait »**, dépend en général de l'initiative de la personne ou l'organisation lésée. Cette procédure peut imposer que la personne ou l'organisation affectée avise directement l'exploitant du site concerné avant que la procédure de retrait du matériel ne puisse être engagée. Si l'exploitant du site refuse de supprimer le matériel jugé illégal, l'autorité compétente du pays peut impartir à l'hébergeur un délai pour supprimer le matériel et/ou peut s'exposer à une responsabilité civile pour le contenu. Les fournisseurs d'accès à internet peuvent même se voir ordonner de bloquer l'accès à l'URL voire l'ensemble du site.

Considérations liées à la liberté d'expression

Si l'on considère les mesures évoquées dans le contexte de la liberté d'expression, une **distinction** entre blocage et retrait de contenu semble pertinente. Le blocage, le filtrage ou la prévention de l'accès à un contenu internet constituent généralement une mesure technique visant à restreindre l'accès à des données ou ressources généralement hébergées dans une autre juridiction. Une telle mesure est en principe prise par le fournisseur d'accès à internet au moyen de matériel informatique ou de logiciels qui bloquent la réception ou l'affichage d'un contenu ciblé spécifique sur les terminaux de ses clients. Quant au retrait ou à la suppression d'un contenu, il consiste pour l'essentiel en une exigence ou en des mesures adressées à l'exploitant du site (ou à l'« hébergeur ») pour qu'il supprime ou efface le contenu ou les pages web incriminés du site. Le blocage est une mesure extrêmement poussée, alors que les dispositions prises à l'encontre d'un hébergeur aux fins de la suppression d'un contenu internet suivent un raisonnement légèrement différent, principalement en termes de proportionnalité.

En matière de blocage, les évolutions récentes concernent principalement deux questions clés : le blocage volontaire et la qualité de la base juridique sur laquelle se fondent les mesures de blocage. Le **blocage volontaire** pose particulièrement problème si (et étant donné que) il est mis en œuvre sans une base juridique, de même qu'il soulève de graves questions quant à la régularité de la procédure. Dans ce contexte, d'aucuns ont fait valoir que les États n'ont pas seulement un devoir de non-ingérence, mais qu'ils ont aussi l'obligation de protéger les libertés fondamentales, et ce notamment en rapport avec les fournisseurs d'accès. Il est intéressant de noter dans ce contexte qu'à compter du 30 avril 2016, le Règlement (UE) 2015/2120 ne permettra pas le blocage volontaire sans une base juridique, notamment (à partir de 2017) un blocage fondé sur l'autoréglementation.

La deuxième question est celle de l'évaluation de la base juridique des mesures de blocage aux termes des critères de l'article 10 de la Convention européenne des droits de l'homme (CEDH). En particulier les bases juridiques établies récemment, mais aussi les changements apportés à des bases juridiques existant depuis

un certain temps (ou à leur application) doivent satisfaire aux critères énoncés à l'article 10, notamment à la question de savoir si le blocage est nécessaire dans une société démocratique pour un but légitime, comme indiqué à l'article 10 (2) de la CEDH. La mesure doit également respecter les limites fixées par le principe de proportionnalité.

S'agissant du **retrait de contenus**, les injonctions directement adressées par une autorité compétente d'un État à un hébergeur aux fins du retrait d'un contenu doivent satisfaire aux conditions énoncées par l'article 10 (2) de la CEDH. Cela vaut pour le cadre juridique national tant général que ciblé. Toutefois, le principal problème dans ce contexte concerne les conséquences qui découlent du fait de tenir l'hébergeur responsable en tant que **co-auteur**, (du moins) s'il a connaissance du contenu illégal. Ce risque de responsabilité pour l'hébergeur pourrait conduire à des excès de suppression. Les procédures de notification et retrait prévues par la loi constituent la meilleure façon d'y remédier. Cependant, ces dispositions sont (encore) relativement rares. Les procédures de notification et retrait autoréglementées ou volontaires, qui existent du moins dans certains domaines dans la plupart des États, n'offrent souvent pas des garanties suffisantes, notamment du point de vue de la régularité de la procédure.

I. Introduction

Le 24 novembre 2014, le Conseil de l'Europe a formellement mandaté l'Institut suisse de droit comparé (« ISDC ») pour réaliser une étude comparative des lois et pratiques en matière de filtrage, blocage et retrait de contenus illégaux sur internet dans ses 47 États membres.

Comme convenu entre l'ISDC et le Conseil de l'Europe, l'étude présente les lois et, pour autant que les informations soient facilement disponibles, les pratiques de filtrage, blocage et retrait de contenus illégaux sur internet dans plusieurs contextes. Elle examine la possibilité de telles mesures en cas de menace à l'ordre public ou à la sécurité intérieure ainsi qu'en cas de violation des droits de la personnalité et des droits de propriété intellectuelle. Dans chaque cas, l'étude examine le cadre juridique qui sous-tend les décisions de filtrer, bloquer ou retirer les contenus illégaux sur internet, l'autorité habilitée à prendre de telles décisions et les conditions d'exécution de ces décisions. Par ailleurs, l'étude se penche sur les possibilités de contrôle extrajudiciaire des contenus en ligne et présente une brève description de la jurisprudence pertinente et importante.

Elle s'organise, pour l'essentiel, en deux parties principales. La première partie consiste en une compilation de rapports nationaux pour chacun des États membres du Conseil de l'Europe. Elle présente une analyse plus détaillée des lois et des pratiques en matière de filtrage, blocage ou retrait des contenus illégaux sur internet dans chaque État membre. Afin de faciliter la lecture et les comparaisons, tous les rapports nationaux sont présentés suivant la même structure (voir ci-dessous, questions). La deuxième partie présente des considérations comparatives sur les lois et les pratiques en matière de filtrage, blocage ou retrait de contenus illégaux en ligne dans les États membres. Elle vise ainsi à faire ressortir et à tenter d'expliquer les convergences et les divergences qui existent le cas échéant entre les approches des États membres sur les questions couvertes par l'étude.

II. Méthodologie et questions

1. MÉTHODOLOGIE

La présente étude a été déployée en trois temps. Dans une première phase, la phase préliminaire, l'ISDC a élaboré un questionnaire détaillé, en coopération avec le Conseil de l'Europe. Une fois approuvé, ce questionnaire (voir point 2 ci-dessous) a servi de base aux rapports nationaux.

La deuxième phase a consisté à produire les rapports pour chaque pays. Cette tâche a été accomplie soit par le personnel de l'ISDC soit par des correspondants externes pour les États que l'Institut ne pouvait pas couvrir en interne. Les principales sources sur lesquelles se sont appuyés les rapports nationaux sont les lois pertinentes et, lorsqu'elles étaient disponibles, les publications académiques sur les questions examinées. En plus, dans certains cas, en fonction de la situation, des entretiens ont eu lieu avec les parties concernées afin de se faire une idée plus précise de la situation. Cela étant dit, les rapports ne sont pas fondés sur des données empiriques et statistiques, dans la mesure où ils visent principalement à analyser le cadre juridique en vigueur.

Dans la phase suivante (la troisième), l'ISDC et le Conseil de l'Europe ont examiné tous les rapports par pays et fourni des informations en retour aux différents auteurs. En plus de cela, l'ISDC a rédigé les commentaires comparatifs sur la base des différents rapports nationaux ainsi que sur la base des publications académiques et des autres ressources disponibles, notamment au Conseil de l'Europe.

Tout au long de ce processus, l'ISDC a coordonné ses activités étroitement avec le Conseil de l'Europe. Cependant, le contenu de l'étude relève de la responsabilité exclusive des auteurs et de l'ISDC. Cela dit, l'ISDC ne peut assumer la responsabilité du caractère complet, correct et exhaustif des informations figurant dans les différents rapports nationaux.

2. QUESTIONS

En accord avec le Conseil de l'Europe, tous les rapports nationaux sont, dans la mesure du possible, structurés suivant les axes ci-après :

1. Quels sont les fondements juridiques des mesures de blocage, filtrage ou retrait des contenus illégaux sur internet ?

Liste indicative de ce que cette partie devrait couvrir :

- ▶ Ce domaine est-il réglementé ?
- ▶ Des normes internationales, notamment des conventions concernant les contenus illégaux sur internet (tels que des conventions sur la protection de l'enfance, la cybercriminalité ou la lutte contre le terrorisme) ont-elles été transposées dans le cadre réglementaire nationale ?
- ▶ Cette réglementation est-elle fragmentée entre plusieurs domaines du droit, ou forme-t-elle plutôt un corpus de règles spécifique à internet ?
- ▶ Présenter un aperçu des sources juridiques qui réglementent les activités de blocage, filtrage ou retrait des contenus illégaux sur internet (une analyse plus détaillée sera présentée dans la réponse à la question 2).

2. Quel est le cadre juridique qui règlemente :

2.1. Le blocage et/ou le filtrage de contenus illégaux sur internet ?

Liste indicative de ce que cette partie devrait couvrir :

- ▶ Pour quels motifs des contenus internet sont-ils bloqués ou filtrés ? Cette partie devrait couvrir tous les motifs suivants, le cas échéant :
 - la protection de la sécurité nationale, l'intégrité territoriale ou la sûreté publique (par exemple, le terrorisme) ;
 - la défense de l'ordre et la prévention du crime (par exemple, la pornographie mettant en scène des enfants) ;

- la protection de la santé publique ou des bonnes mœurs;
- la protection de la réputation ou des droits d'autrui (par exemple, les droits relatifs à la diffamation, à la vie privée ou à la propriété intellectuelle);
- la prévention de la diffusion d'informations confidentielles.
- ▶ Quelles exigences et garanties le cadre juridique énonce-t-il pour un tel blocage ou filtrage ?
- ▶ Quel est le rôle des fournisseurs d'accès à internet dans la mise en œuvre de ces mesures de blocage et de filtrage ?
- ▶ Existe-t-il des instruments juridiques non contraignants (meilleures pratiques, codes de conduite, lignes directrices, etc.) dans ce domaine ?
- ▶ Une description concise de la jurisprudence pertinente.

2.2. Le retrait ou la suppression de contenus illégaux sur internet ?

Liste indicative de ce que cette partie devrait couvrir :

- ▶ Pour quels motifs des contenus internet sont-ils retirés ou supprimés ? Cette partie devrait couvrir tous les motifs suivants, le cas échéant :
 - la protection de la sécurité nationale, l'intégrité territoriale ou la sûreté publique (par exemple, le terrorisme);
 - la défense de l'ordre et la prévention du crime (par exemple, la pornographie mettant en scène des enfants);
 - la protection de la santé publique ou des bonnes mœurs;
 - la protection de la réputation ou des droits d'autrui (par exemple, les droits relatifs à la diffamation, à la vie privée ou à la propriété intellectuelle);
 - la prévention de la diffusion d'informations confidentielles.
- ▶ Quel est le rôle des fournisseurs d'hébergement sur internet et des médias sociaux et autres plateformes (réseaux sociaux, moteurs de recherche, forums, blogs, etc.) dans la mise en œuvre de ces mesures de retrait ou de suppression de contenus ?
- ▶ Quelles exigences et garanties le cadre juridique énonce-t-il pour une telle suppression ?
- ▶ Existe-t-il des instruments juridiques non contraignants (meilleures pratiques, code de conduite, lignes directrices, etc.) dans ce domaine ?
- ▶ Description concise de la jurisprudence pertinente.

3. Aspects procéduraux : quels sont les organes habilités à décider du blocage, filtrage ou retrait de contenus internet ? Comment la mise en œuvre de ces décisions est-elle organisée ? Des possibilités de révision sont-elles prévues ?

Liste indicative de ce que cette partie devrait couvrir :

- ▶ Quels sont les organes (judiciaires ou administratifs) habilités à décider du blocage, filtrage ou retrait de contenus illégaux sur internet ?
- ▶ Comment ces décisions sont-elles mises en œuvre ? Décrire les étapes de la procédure jusqu'au blocage, filtrage ou retrait effectif du contenu internet incriminé.
- ▶ Quelles sont les obligations de notification de la décision aux individus ou parties concernés ?
- ▶ Les parties concernées ont-elles la possibilité de solliciter et d'obtenir la révision d'une telle décision par un organe indépendant ?

4. La surveillance générale d'internet : existe-t-il dans votre pays une entité responsable de la surveillance des contenus internet ? Dans l'affirmative, sur quelle base cette activité de surveillance est-elle mise en œuvre ?

Liste indicative de ce que cette partie devrait couvrir :

- ▶ Il s'agit ici des entités chargées de contrôler les contenus internet et d'évaluer leur conformité avec les prescriptions légales, y compris les droits de l'homme – il peut s'agir d'entités spécifiques responsables d'un tel contrôle ainsi que des fournisseurs de services internet. De telles entités existent-elles ?

- ▶ Quels critères d'évaluation des contenus internet appliquent-elles ?
- ▶ De quels pouvoirs disposent-elles pour s'attaquer aux contenus illégaux sur internet ?

5. Évaluation de la jurisprudence de la Cour européenne des droits de l'homme

Liste indicative de ce que cette partie devrait couvrir :

- ▶ La législation régissant le blocage, filtrage ou retrait de contenus internet satisfait-elle aux exigences de qualité (prévisibilité, accessibilité, clarté et précision) énoncées par la Cour européenne des droits de l'homme ? Existe-t-il des garanties pour la protection des droits de l'homme (notamment la liberté d'expression) ?
- ▶ La législation inclut-elle les garanties nécessaires pour prévenir l'abus de pouvoir et l'arbitraire conformément aux principes établis par la jurisprudence de la Cour européenne des droits de l'homme (par exemple, la garantie que les décisions de blocage ou de filtrage sont aussi ciblées que possible et ne sont pas utilisées comme un moyen de blocage à grande échelle) ?
- ▶ Les prescriptions légales sont-elles respectées dans la pratique, notamment pour ce qui est de l'évaluation de la nécessité et de la proportionnalité de toute ingérence dans l'exercice de la liberté d'expression ?
- ▶ En cas d'existence d'un cadre d'autoréglementation dans ce domaine, est-il assorti de garanties de protection de la liberté d'expression ?
- ▶ La jurisprudence pertinente est-elle en conformité avec la jurisprudence pertinente de la Cour européenne des droits de l'homme ?

Dans certains rapports nationaux, cette partie reflète principalement des publications académiques nationales ou internationales sur ces questions dans l'État concerné. Dans d'autres rapports, les auteurs font une évaluation plus indépendante.

IV Considérations comparatives

TABLE DES MATIERES

1. MODÈLES NATIONAUX POUR LA RÉGLEMENTATION DU BLOPAGE, FILTRAGE ET RETRAIT DE CONTENUS ILLÉGAUX SUR INTERNET	12
1.1. Blocage, filtrage et retrait de contenus illégaux sur internet en l'absence de cadre législatif national spécifique	12
1.2. Blocage, filtrage et retrait de contenus en ligne dans un cadre législatif national ciblé	13
1.2.1. Motifs invoqués pour le blocage, le filtrage et le retrait de contenus sur internet	13
1.2.2. Mécanismes procéduraux	17
2. ASPECTS DES DROITS DE L'HOMME LIÉS AU BLOPAGE ET À L'HÉBERGEMENT	18
2.1. Blocage et filtrage par des FSI	19
2.1.1. Problématique	19
2.1.2. Les exigences relatives à l'existence d'une base légale pour le blocage et la Cour européenne des droits de l'homme	20
2.1.3. Base juridique et blocage volontaire et le Conseil de l'Europe	22
2.1.4. Développements dans l'UE concernant la base légale et le blocage volontaire	23
2.1.5. Evaluation	27
2.2. Retrait de contenus par un hébergeur	29
2.2.1. Retrait et blocage : subsidiarité	29
2.2.2. Trois approches de base pour le retrait et leurs implications en matière de droits de l'homme	29
2.2.3. Une évaluation axée sur les droits de l'homme des approches concernant les activités d'hébergeur	32

Cette partie présente les modèles nationaux les plus courants de régulation du blocage, du filtrage et du retrait de contenus illégaux sur internet, avec une analyse de leurs conséquences en matière de liberté d'expression.

Cette partie, qui présente un **panorama général des principaux cadres réglementaires nationaux** identifiés par l'étude, mettra l'accent sur les grandes problématiques liées à la liberté d'expression et permettra aussi de faciliter la compréhension des rapports pays. Les observations et commentaires rapportés reposent sur des constats (dont ils s'inspirent) pour chaque État membre du Conseil de l'Europe, cependant il ne sera fait référence qu'aux pays les plus caractéristiques, et à titre d'exemple. De plus, la recherche a révélé que, si certains pays peuvent être rattachés à une catégorie particulière de « modèle » réglementaire, les principes, approches et mesures relevés sont si variés qu'il n'est pas possible, dans le cadre du mandat actuel, de faire un commentaire comparatif exhaustif.

Cette **synthèse comparative est articulée en deux volets** : le premier examine les différents modèles identifiés pour les problématiques liées au blocage, au filtrage et à la suppression de contenus illégaux en ligne, et le second analysera ces mesures et en évaluera l'impact sur la liberté d'expression.

On va voir que le blocage et le retrait (ou « suppression ») de contenus en ligne sont souvent traités de manière similaire par les États examinés ou, pour les pays dotés de cadres législatifs ciblés, par les mêmes ensembles de règles.

Ces termes ne devraient toutefois pas être confondus entre eux. Dans ce premier volet, par **blocage, filtrage ou prévention de l'accès à des contenus sur internet**, on entendra en général des mesures techniques visant à restreindre l'accès à des informations ou ressources le plus souvent hébergées dans une autre juridiction. Ces actions sont en général menées par le fournisseur d'accès à l'internet grâce à des produits logiciels ou matériels qui bloquent des contenus ciblés et les empêchent d'être reçus ou affichés sur les dispositifs de ses clients. Un certain nombre de techniques peuvent être employées, par exemple le blocage du DNS (Système de noms de domaine - *Domain Name System*) ou de l'URL (*Uniform Resource Locator*). **La suppression ou le retrait de contenus en ligne**, en revanche, couvre de manière générale des demandes ou mesures concernant l'opérateur du site web (ou « hébergeur ») afin que celui-ci retire ou supprime les contenus en ligne ou pages web litigieux. Les fournisseurs d'accès à l'internet et les hébergeurs peuvent tous deux être considérés comme des « intermédiaires d'internet ».

1. MODÈLES NATIONAUX POUR LA RÉGLEMENTATION DU BLOCAGE, FILTRAGE ET RETRAIT DE CONTENUS ILLÉGAUX SUR INTERNET

Pour ce qui est du blocage, du filtrage et du retrait de contenus illégaux sur internet, deux catégories générales de « modèle » réglementaire national ont été identifiées à l'issue de la recherche.

La première regroupe les **pays qui n'ont pas de législation spécifique** sur la question, et où ces actes sont réglementés par référence à la législation générale ou entrepris par d'autres acteurs non-étatiques ou étatiques (voir analyse en partie 1.1).

La deuxième couvre des **pays où l'on peut dire que le législateur est « intervenu » pour établir un cadre juridique** dans lequel sont exécutées des mesures de blocage, de filtrage et de retrait. Les pays dans ce cas se sont dotés d'approches et d'outils aussi divers que variés qui seront analysés dans la partie 1.2.

1.1. Blocage, filtrage et retrait de contenus illégaux sur internet en l'absence de cadre législatif national spécifique

Un nombre significatif de pays ne disposent pas de cadre juridique spécifique pour le blocage, le filtrage et le retrait de contenus illégaux sur internet. En d'autres termes, il n'y a pas de système législatif ou autre mécanisme réglementaire mis en place par l'État pour définir les conditions et procédures à respecter par ceux qui prennent des mesures de blocage, de filtrage ou de retrait de contenus sur internet.

En l'absence de cadre juridique spécifique ou ciblé, **plusieurs pays s'appuient sur un cadre juridique « général » qui n'est pas spécifique à internet** pour mener ce qui, pour dire les choses de manière générale, constitue des actions de blocage ou de retrait de contenus illégaux en ligne. Tel est le cas de l'Allemagne, de l'Autriche, des Pays-Bas, du Royaume-Uni, de l'Irlande, de la Pologne, de la République tchèque et de la Suisse où les législateurs nationaux ont en effet choisi de s'abstenir d'adopter un cadre législatif ciblé pour des mesures de réglementation permettant le blocage, le filtrage et le retrait de contenus sur l'internet.

La portée de l'absence de réglementation varie cependant d'un pays à l'autre. De plus, diverses raisons expliquent ce **manque d'intervention délibéré** de la part de l'État. Dans certaines juridictions, notamment la République tchèque et la Pologne, on peut dire que le législateur a décidé que les situations spécifiques à l'internet peuvent être règlementées par des dispositions de nature plus générale – qui de fait n'avaient jamais été expressément prévues pour s'appliquer à des contenus en ligne. Un autre argument souvent invoqué dans ce contexte est l'impossibilité pour le législateur de suivre le rythme des évolutions technologiques.

Les raisons sous-jacentes à l'absence d'activité législative peuvent également trouver leur source dans les **traditions juridiques d'un pays** donné. Certains États, comme le Royaume-Uni et d'autres pays de *Common law* examinés dans le cadre de cette étude n'ont pas adopté de cadre juridique global visant à règlementer internet, préférant au contraire que la plupart des problèmes soient réglés par la régulation volontaire au moyen d'une coopération avec le secteur privé. D'autres pays, tels que les Pays-Bas, préfèrent suivre une approche où les tribunaux élaborent des solutions pragmatiques pour résoudre les points litigieux. En Suisse, en revanche, jusqu'à récemment, le pays n'a pas jugé impératif d'adopter des dispositions spécifiques pour le blocage, le filtrage et le retrait de contenus sur internet.

Toutefois, à mesure que ces pays sont de plus en plus confrontés à la réalité de litiges liés au contenu sur internet, l'absence d'intervention législative présente des difficultés. Ces dernières années, il a été recouru à des **mécanismes divers, et souvent innovants, pour combler la lacune réglementaire** et traiter des points spécifiques. Certaines juridictions ont même choisi de combiner les approches, conservant un cadre en grande partie non règlementé, mais assorti d'interventions législatives et politiques dans certains secteurs bien délimités.

Dans certaines juridictions, **le secteur privé a adopté l'autorégulation** pour combler la lacune due au choix du législateur de ne pas intervenir dans le domaine en jeu. De nombreuses juridictions ont encouragé le secteur privé à adopter et mettre en œuvre des codes de conduite pour internet. De manière générale, cette approche a habituellement pour but de compléter un ensemble de règles plus larges qui forment un cadre juridique spécifique relatif au blocage, au filtrage et au retrait de contenus illégaux en ligne. Toutefois, dans certaines juridictions, comme le Royaume-Uni, le blocage, le filtrage et le retrait de contenus illégaux sur internet se fait largement par le biais d'une réglementation privée, soit par l'application des politiques des intermédiaires de l'internet relatives aux conditions d'utilisation, soit par coopération volontaire des fournisseurs de services internet (qu'ils soient fournisseurs d'accès ou hébergeurs) avec la police et d'autres autorités, accompagnée de règles législatives dans des secteurs spécifiques, par exemple le retrait de contenu terroriste et des procédures de notification et retrait concernant des contenus diffamatoires. Dans d'autres États, tels que la Suisse, des mesures de blocage pour certains types de contenus en ligne ne sont mises en œuvre qu'après un dialogue entre l'autorité administrative compétente et les fournisseurs d'accès à internet.

Dans d'autres pays, ce sont les **juridictions nationales** qui sont chargées de veiller à ce qu'un équilibre soit trouvé entre la liberté d'expression d'une part et la sécurité sur internet et la protection maximale possible d'autres droits fondamentaux d'autre part. Telle est par exemple la situation aux Pays-Bas ainsi que, dans une moindre mesure, en Allemagne.

1.2. Blocage, filtrage et retrait de contenus sur internet dans un cadre législatif national ciblé

Dans bon nombre de juridictions, le législateur est intervenu pour instaurer **un cadre juridique spécifiquement adapté à la réglementation de l'internet et d'autres médias numériques**, notamment pour le blocage, le filtrage et le retrait de contenus en ligne. Il est ressorti de l'étude que ce type de législation définit en général les motifs juridiques sur lesquels une ordonnance de blocage ou de retrait peut être délivrée, l'autorité administrative ou judiciaire qui a compétence pour prendre l'action nécessaire et les procédures à suivre. Ces éléments sont examinés dans cette partie.

1.2.1. Motifs invoqués pour le blocage, le filtrage et le retrait de contenus sur internet

Dans les pays où le législateur a choisi d'établir un cadre juridique ciblé, ce dernier **définira en général les motifs et conditions spécifiques** permettant l'exécution d'un blocage, d'un filtrage ou d'un retrait de contenus sur internet. Dans plusieurs pays, la législation équilibre les intérêts opposés en jeu avant les décisions et permet de rendre une ordonnance de retrait ou de suppression lorsqu'un intérêt spécifique est violé (démonstration du préjudice). Dans d'autres, l'équilibrage entre les intérêts qui s'opposent incombe aux tribunaux.

De manière générale, les motifs invoqués correspondent dans les grandes lignes **aux intérêts protégés par l'article 10 (2) de la Convention européenne des droits de l'homme** (CEDH), à savoir la protection de la sécurité nationale, de l'intégrité territoriale ou de la sûreté publique, la défense de l'ordre et la prévention du crime, la protection de la santé ou de la morale, la protection de la réputation ou des droits d'autrui, et la prévention de la divulgation d'informations confidentielles.

Aux fins de la présente étude, **quatre grandes catégories de motifs juridiques** pouvant être invoqués pour l'adoption de mesures de blocage, de filtrage et de retrait de contenus sur internet ont été identifiées : la protection de la santé et de la morale, notamment la lutte contre les sites web contenant des contenus pédopornographiques ou des sites web illégaux de paris en ligne, la protection de la sécurité nationale, de l'intégrité territoriale ou de la sûreté publique, y compris les actions de contre-terrorisme, la protection des droits de propriété intellectuelle et la protection à l'encontre de la diffamation et du traitement illégal de données à caractère personnel. Différents États définissent le discours de haine de manière différente, ce qui peut donc relever de différentes catégories de motifs juridiques en fonction du pays concerné.

La manière dont les États dotés d'un tel cadre juridique définissent les motifs et conditions spécifiques pour le blocage, le filtrage et le retrait de contenus sur internet varie cependant considérablement. Alors que les motifs les plus communs pour l'adoption de mesures de blocage, de filtrage et de retrait sont exhaustifs et expressément définis dans la législation de la plupart des pays souscrivant à un tel modèle réglementaire, certaines juridictions ont, dans les faits, étendu les motifs pour lesquels il est possible légitimement d'entreprendre un blocage ou retrait – souvent par modification de la législation ou par une interprétation judiciaire créative. Certains exemples vont être mentionnés plus bas, mais cette partie se concentre sur les motifs et conditions habituellement invoqués par les pays examinés.

1.2.1.1. Protection de la santé publique ou de la morale

Les mesures les plus communes relevées au titre de la protection de la morale ou de la santé publique sont celles qui visent spécifiquement la protection contre **les abus sexuels à l'encontre des enfants et les paris illégaux en ligne**. De tels motifs ont été retrouvés largement dans toutes les juridictions examinées et, en particulier pour ce qui est des abus sexuels à l'encontre des enfants, peuvent être attribués, au sein des États de l'UE du moins, à la mise en œuvre de la Directive 2011/92/UE relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants ainsi que la pédopornographie, qui remplace la Décision-cadre 2004/68/JAI du Conseil.

Certaines juridictions, cependant, vont au-delà des motifs habituellement invoqués pour autoriser des mesures de blocage et de retrait en vue de protéger la morale et la santé publique. Tel est le cas, par exemple, de la Fédération de Russie où la diffusion d'informations contenant des propos obscènes, la pornographie (non infantine) et la « propagande homosexuelle » sont également sur la liste des contenus en lignes qui peuvent légitimement faire l'objet de mesures de blocage et de retrait. De même, le cadre juridique turc permet des mesures de blocage, de filtrage et de retrait à l'encontre de contenus sur internet qui sont obscènes, qui font la promotion de la prostitution ou qui facilitent l'usage de stupéfiants.

(a) Pédopornographie

Les mesures restrictives adoptées en lien avec les abus sexuels en ligne à l'encontre des enfants couvrent notamment des ordonnances de blocage ainsi que de retrait des contenus délictueux, en fonction des possibilités techniques et de l'autorité compétente pour ordonner de telles mesures. Il existe **des différences considérables dans la manière dont ces mesures sont mises en œuvre**.

Dans certains pays examinés, tels que l'Espagne et Chypre, ce sont les tribunaux **qui sont responsables de la délivrance d'ordonnances de blocage de contenus en ligne pédopornographiques**. Dans certaines juridictions, telles que le Portugal, un système hybride a été mis en place : une autorité administrative indépendante s'est vue chargée de mettre en œuvre des mesures de blocage temporaire avant l'obtention d'une autorisation judiciaire délivrée par des tribunaux.

Dans d'autres pays, notamment la Belgique et l'Italie, **le procureur ou le juge d'instruction** jouent un rôle important dans l'adoption de mesures de blocage ou de retrait. En Italie, le procureur doit autoriser la liste des contenus illégaux avant que l'on puisse procéder au blocage ou au retrait, alors qu'en Belgique, c'est la prérogative du procureur ou du juge d'instruction qui seuls peut ordonner les mesures de blocage ou de retrait dans le contexte de l'enquête pertinente concernant le contenu illégal.

D'autres juridictions ont mis en œuvre une possibilité de **blocage administratif par une autorité publique** : tel est le cas de la Fédération de Russie, de la Turquie ainsi que de l'Albanie où l'autorité publique de surveillance de l'internet peut rendre des ordonnances pour de telles mesures. La France a adopté un système hybride

où les services de police compétents en matière d'internet peuvent adopter des mesures de blocage ou de retrait de contenus liés à des délits pénaux tels que la pédopornographie, sous la supervision d'une autorité administrative indépendante chargée de garantir la liberté de l'internet.

Dans d'autres juridictions, par exemple la Finlande, certains intermédiaires d'internet ont une responsabilité spécifique, **même en l'absence d'ordonnance judiciaire**, les obligeant à agir dès lors qu'ils ont connaissance de contenus manifestement illégaux, notamment en cas de pornographie infantine.

(b) Paris illégaux en ligne

Dans le domaine des paris illégaux en ligne, plusieurs pays prévoient des mesures de blocage et de retrait concernant les sites proposant ce type d'activité qui n'ont pas obtenu d'agrément dans leur juridiction. Le choix de bloquer ou de retirer le contenu litigieux dépendra généralement de la localisation de l'hébergeur du site web concerné. Dans la plupart des pays, **ces mesures restrictives sont prises à l'initiative de l'autorité publique** compétente pour surveiller les activités des paris illégaux. Tel est par exemple le cas en Belgique, en France, en Turquie, dans la Fédération de Russie et à Chypre. Dans bon nombre de juridictions, on ne sait pas clairement dans quelle mesure une autorité administrative de ce genre est indépendante des organes de l'État.

La **mise en œuvre de l'ordonnance** est assurée par les fournisseurs d'accès internet nationaux, que ce soit du fait d'un accord de coopération avec l'autorité publique de surveillance (en Belgique), du fait d'une ordonnance d'un tribunal (comme en France ou en Turquie où les tribunaux sont également compétents) ou en réponse à une ordonnance administrative, comme on l'a vu dans des pays tels que la Turquie, la Fédération de Russie et Chypre.

1.2.1.2. Contre-terrorisme et sûreté nationale

Bon nombre des pays étudiés **se sont dotés de mécanismes spécifiques** pour bloquer, filtrer ou retirer du contenu sur internet lié à des activités terroristes ou qui peuvent porter atteinte sous une forme ou une autre à la sûreté nationale. Pour les États dont les cadres juridiques octroient expressément à des institutions des compétences pour ordonner aux hébergeurs et fournisseurs de services internet de prendre de telles mesures, la source de ces règles de droit varie.

Certains pays, tels que la Turquie, l'Espagne et la France, ont dressé une liste dans les catégories d'activités prohibées qui sont assorties d'un **dispositif législatif unique visant spécifiquement le blocage et le retrait de contenu sur internet**. Les dispositions d'application qui confèrent aux organes pertinents le pouvoir d'agir peuvent figurer dans la législation elle-même (par exemple dans le cas de la France et de la Turquie) ou être incluses dans les codes pénaux ou autres textes législatifs dans lesquels l'activité illégale en question est plus largement règlementée (par exemple, dans le Code pénal espagnol).

D'autres pays ont adopté des **textes législatifs s'appliquant directement au contre-terrorisme** et contenant des dispositions pour le blocage et le retrait de contenus à visées terroristes. Ces dispositions peuvent, comme pour la Russie, venir en parallèle à d'autres dispositions législatives ciblées concernant le blocage et le retrait de contenu illégal, mais elles servent à prévoir des procédures spécifiques pour le retrait de contenus à visées terroristes. Toutefois, même certains pays qui ne se sont pas dotés d'un cadre juridique ciblé pour traiter le retrait de contenus litigieux sur internet peuvent envisager que le contre-terrorisme mérite une réglementation législative particulière. On le voit, par exemple, dans la loi de 2006 du Royaume-Uni contre le terrorisme qui contient des dispositions spécifiques pour le retrait et la suppression de contenu de ce type.

Bon nombre de pays adoptent **des définitions larges de ce que sont les activités illégales** pour lesquelles des mesures de blocage sur internet peuvent trouver à s'appliquer. Ainsi, des contenus ayant potentiellement des fins terroristes peuvent être retirés ou bloqués en vertu de dispositions plus larges protégeant « l'ordre public », « la sécurité publique » ou encore « la défense nationale » ou, comme c'est le cas en Belgique, des comportements « contraires à la morale » ; d'autres font référence spécifiquement aux contenus qui « incitent à des actes de terrorisme ou en font l'apologie ». L'un des pays significatifs de ce point de vue est la Fédération de Russie dont la loi fédérale pour contrer les activités extrémistes identifie une large gamme d'activités décrites comme « extrémistes » pour lesquelles les contenus associés sur internet peuvent être bloqués ou retirés. Ces « contenus extrémistes » sont très largement définis et peuvent couvrir des contenus liés à des activités terroristes, mais aussi à « l'atteinte à la dignité nationale » et à « l'incitation à des troubles de masse ».

Parmi les pays disposant de cadres législatifs ciblés, il est fréquent que des ordonnances de blocage ou de retrait **puissent être rendues à la fois par des autorités administratives désignées et par un tribunal pertinent sur requête**. Tel est le cas en Russie et en France où les autorités administratives ou les organes policiers pertinents ont les compétences requises pour exiger le blocage ou le retrait de contenus délictueux sans qu'il soit nécessaire d'obtenir pour cela une ordonnance judiciaire. En Turquie, contrairement aux dispositions

relatives au blocage pour d'autres contenus délictueux sur internet, le Premier ministre et d'autres ministres au gouvernement peuvent eux-mêmes demander le blocage ou le retrait en cas d'urgence. D'autres systèmes juridiques, par exemple celui de l'Espagne, exigent une décision judiciaire ou une confirmation judiciaire de la décision de l'organisme administratif compétent avant que le retrait puisse avoir lieu.

1.2.1.3. Protection des droits de la propriété intellectuelle

Conformément à l'article 8 (2) de la Directive de l'UE sur la société de l'information, les États membres de l'UE ont traduit en droit interne les **mesures nécessaires pour garantir que les titulaires de droits de propriété intellectuelle violés** puissent saisir les tribunaux nationaux pour obtenir des ordonnances à l'encontre des intermédiaires sur internet afin que le contenu litigieux soit retiré ou bloqué. Des règles législatives spécifiques, habituellement intégrées dans une législation plus large relative au droit de la propriété intellectuelle, permettent en général cette compétence judiciaire, même dans des pays tels que l'Allemagne, la Suède et le Royaume-Uni où il n'existe par ailleurs pas de règle ciblée sur le blocage et le retrait de contenu sur internet en général.

En revanche, les pays dotés de cadres législatifs spécifiques pour le blocage et le retrait de contenus illégaux en ligne disposent souvent de règles claires sur **les sauvegardes à prendre en compte lorsqu'on envisage un retrait**. Ainsi, la loi espagnole sur la propriété intellectuelle prévoit le retrait et la suspension de contenus qui violent des droits de la propriété intellectuelle, mais d'autres textes législatifs sur les services de la société de l'information qui régissent spécifiquement le retrait de contenus en ligne fixent les normes, les sauvegardes et les procédures qui doivent être respectées chaque fois que des mesures restrictives sont appliquées.

Dans les pays disposant de textes législatifs ciblés pour le blocage et le retrait de contenus en ligne, **on a trouvé également plus de règles spécifiques détaillées visant les intermédiaires en ligne concernant des aspects des droits de propriété intellectuelle** qui vont au-delà du droit d'auteur et couvrent par exemple les brevets et les marques. Alors que les tribunaux dans d'autres pays doivent appliquer des principes et des procédures liés à la délivrance d'ordonnances au titre des lois générales relatives à la propriété intellectuelle, dans des systèmes juridiques tels que ceux de la France et de la Finlande, il existe des règles spécifiques liées à des mesures restrictives à l'encontre d'intermédiaires sur internet dans ces branches du droit de la propriété intellectuelle. Par rapport aux contenus publiés sous des formes plus traditionnelles, ces règles reconnaîtront de manière générale les spécificités du contenu en ligne, telles que le rôle de l'intermédiaire sur internet par rapport à l'auteur du contenu en question.

1.2.1.4. Protection de la réputation et des données à caractère personnel

Les droits individuels ou relatifs à la vie privée sont **définis et traités différemment en fonction des pays examinés**. Ils peuvent couvrir la protection de la réputation ou contre la diffamation, la protection des données à caractère personnel et d'autres violations de la vie privée. Les mécanismes légaux pour le blocage et le retrait de contenus portant atteinte à ces droits individuels varient, même entre les pays dotés d'un cadre juridique qui prévoit spécifiquement le retrait de contenus illégaux en ligne.

Dans de nombreux pays, le retrait de ce type de contenus en ligne s'effectue **dans le cadre de règles générales visant à sanctionner les violations du droit à la protection de la vie privée ou de droits de la personne**. Dans d'autres, la base légale pour le retrait peut émaner d'une législation ou de codes spécifiques applicables au retrait de contenus en ligne préjudiciables ou dommageables à l'égard d'une personne physique ou morale. La France est l'un des exemples de pays qui prévoient les deux possibilités. Parmi les pays de l'UE très certainement, ainsi que pour les États parties à la Convention 108 du Conseil de l'Europe, la mise en œuvre du cadre européen ou international au niveau national signifie que les pays ont déjà mis en place des règles visant généralement le retrait de données à caractère personnel qui violent les principes de protection des données. Ces règles ont été utilisées pour exiger des intermédiaires d'internet qu'ils retirent les contenus, étant donné qu'ils peuvent être considérés comme des acteurs du traitement de données impliqués dans le traitement de contenus délictueux.

La Russie et la Turquie sont des exemples de pays qui ont mis en œuvre des règles relatives à la protection des données à caractère personnel et à la protection de la vie privée **spécifiquement adaptées au retrait de données en ligne**. Ces règles permettent en général à quiconque de demander une ordonnance à l'encontre d'opérateurs de sites web et de fournisseurs d'accès à internet afin que ceux-ci retirent le contenu qui viole les principes de protection des données.

La protection contre la diffamation et la protection des autres droits liés à la protection de la réputation sont souvent traitées au pénal ou au civil et parfois dans les deux. Les ordonnances visant à bloquer les contenus offensants peuvent être délivrées par des tribunaux dans le cadre des procédures judiciaires du

pays concerné, mais bon nombre de pays prévoient maintenant également des ordonnances pour le retrait ou le blocage de contenu illégal qui peuvent être délivrées à l'encontre de l'intermédiaire de l'internet, sans qu'il soit nécessaire d'avoir intenté des procédures civiles ou pénales à l'encontre de l'auteur de ce contenu. Ces pays proposent souvent des procédures de retrait accéléré du contenu litigieux qui vont plus vite que la procédure habituelle via la saisine d'un tribunal.

Dans la plupart des pays, ce sont les **tribunaux qui sont l'autorité de dernier recours pour ordonner le retrait et le blocage de contenus sur internet** présumés violer les droits liés à la protection de la vie privée. Tel est le cas pour des pays qui opèrent selon des règles spécifiques relatives au retrait et au blocage de contenus en ligne, ainsi que pour ceux qui ne disposent pas d'un cadre juridique ciblé et où les personnes lésées doivent de manière générale obtenir des ordonnances délivrées par des juges au titre des dispositions légales générales. Toutefois, en France, en Russie et en Turquie par exemple, des **autorités administratives sont dotées de pouvoirs considérables** pour exiger le retrait de contenus violant les droits relatifs à la protection de la vie privée, en particulier dans le domaine de la protection des données. Elles peuvent même avoir le droit, dans certains cas, d'ordonner à un intermédiaire de l'internet de supprimer ou de bloquer l'accès à des contenus litigieux sans qu'il soit nécessaire d'obtenir au préalable l'intervention d'une autorité judiciaire.

1.2.2. Mécanismes procéduraux

Dans tous les pays examinés, les procédures suivies en matière de blocage et de retrait de contenus en ligne sont spécifiques en fonction du système juridique et de la nature des contenus concernés. On peut néanmoins relever un certain nombre de pratiques communes.

Concernant **les contenus à nature pédopornographique, à visées terroristes, criminels (en particulier les crimes de haine) et menaçant la sécurité nationale**, bon nombre des États ayant des dispositions légales ciblées pour le retrait de contenu en ligne prévoient le blocage urgent de ce type de contenus sans qu'il soit nécessaire d'obtenir au préalable une ordonnance judiciaire. Tel est le cas dans des pays tels que la Russie, la France et la Turquie. **Les autorités administratives, services de police ou procureurs sont dotés de pouvoirs spécifiques** pour ordonner aux fournisseurs d'accès à l'internet le blocage de l'accès sans nécessité d'une ordonnance judiciaire préalable. On voit communément ce type d'ordonnance exigeant de la part du fournisseur d'accès à internet qu'il agisse dans les 24 heures, et sans aucune notification aux fournisseurs de contenus ou à l'hébergeur. Dans d'autres pays, tels que la Finlande, une ordonnance judiciaire est nécessaire ; il est attendu des fournisseurs de services d'hébergement ayant connaissance de l'existence de ce type de contenus en ligne de les retirer volontairement sans ordonnance judiciaire et de le notifier aux fournisseurs de contenu, ce qui permet ensuite à ce dernier de contester l'action devant les tribunaux.

Un certain nombre de systèmes nationaux exigent de l'autorité administrative compétente qu'elle **obtienne la validation judiciaire subséquente pour l'ordonnance rendue** (tel est le cas en Turquie lorsque des contenus en ligne sont considérés comme constituant une menace pour la sécurité nationale et l'ordre public), d'autres plaçant une page spéciale (*splash*) à l'endroit du matériel bloqué expliquant pourquoi le contenu est bloqué et comment il est possible de contester la décision. Dans la majeure partie des pays, les parties intéressées ont **la possibilité de contester des actions de blocage selon les voies de recours normales de la procédure pénale (ou, au besoin, civile).**

En particulier pour ce qui est de contenus concernant la pédopornographie et d'autres crimes graves, de nombreux pays (tels que la France, la Russie et le Royaume-Uni) recourent à un **système de «liste»** où une liste centrale des URL et noms de domaine bloqués est conservée et mise à jour par l'autorité administrative compétente. Elle est notifiée aux fournisseurs d'accès à internet concernés qui ont l'obligation de garantir que le blocage est appliqué. **Ces listes sont mises à jour de manière régulière, parfois même toutes les heures, et périodiquement passées en revue** pour déterminer si le blocage est encore nécessaire ou si les contenus en question ont été par la suite retirés. Dans certains pays, comme la Finlande, certaines ordonnances de blocage peuvent expirer après un certain laps de temps si aucune action n'a été intentée au civil ou au pénal concernant le contenu.

Dans bon nombre d'États, le retrait et le blocage de **contenus qui violent les droits de la propriété intellectuelle, les droits de la protection de la vie privée et de contenus diffamatoires** sont effectués ou autorisés **uniquement sur ordonnance judiciaire.**

Même dans des pays tels que l'Espagne qui dispose d'une autorité administrative dotée des pouvoirs nécessaires pour exiger le retrait de **contenus qui violent les intérêts de la propriété intellectuelle**, il est nécessaire que cet acte soit autorisé par ordonnance judiciaire. Il est possible ensuite de faire appel de cette décision conformément aux procédures civiles (et, en tant que de besoin, pénales) habituelles. Certains pays ont introduit

des procédures alternatives de notification et de retrait conçues pour éviter de recourir aux tribunaux. Dans le cadre du nouveau Code finlandais sur la société de l'information, par exemple, une procédure a été établie pour que les détenteurs de droits d'auteur puissent obtenir le retrait de contenu réputé illégal, sous réserve que les fournisseurs de contenus puissent bénéficier d'un droit de recours afin de contester le retrait.

En ce qui concerne les **droits liés à la protection contre la diffamation et à la protection de la vie privée**, étant donné que leur application dépendra en général du déclenchement par la personne lésée (la « victime ») d'une action pour les faire valoir, bon nombre de pays proposent **sous une forme ou une autre une procédure de « notification et retrait »**. Dans le cadre de cette procédure, la victime peut avoir à notifier directement l'opérateur du site web concerné avant que les procédures de retrait du contenu contesté puissent être entamées. Lorsque ce dernier refuse de retirer les contenus jugés illégaux, l'autorité nationale pertinente peut fixer une échéance à l'hébergeur pour s'exécuter qui, si elle n'est pas respectée, peut même donner lieu à une ordonnance à l'égard des fournisseurs d'accès à internet pour que ceux-ci bloquent l'accès à l'URL, voire même à l'intégralité du site web. On trouvera ce type de règles, par exemple, en Turquie et en Russie.

Dans d'autres juridictions, telles que la France et Monaco, si l'intermédiaire d'internet concerné a été formellement notifié par le détenteur des droits de l'existence de contenu potentiellement illégal et n'a pas agi, cela peut **avoir des conséquences pour l'engagement de la responsabilité de l'intermédiaire en tant que tiers**. En France, le fait pour un opérateur de site web de ne pas retirer des contenus *manifestement illégaux* en matière de droit de la propriété intellectuelle peut entraîner l'engagement d'une responsabilité conjointe. De même, au Royaume-Uni, où il n'y a pas de cadre plus large sur le retrait et le blocage de contenus en ligne, les opérateurs de sites web ne peuvent bénéficier de l'exonération de responsabilité automatique pour déclarations diffamatoires en cas d'action intentée ultérieurement au civil s'ils n'ont pas agi à la suite d'une notification légale et dans le cadre de procédures de retrait.

2. ASPECTS DES DROITS DE L'HOMME LIÉS AU BLOCAGE ET À L'HÉBERGEMENT

Du point de vue de l'article 10 de la CEDH, une ordonnance par une autorité publique ou un juge à l'encontre d'un fournisseur d'accès à internet (ou hébergeur) afin qu'il bloque (ou retire) des contenus constitue une ingérence claire dans la liberté d'expression. Dans certains de ses arrêts, la Cour européenne des droits de l'homme a conclu que les discours de haine ou l'expression d'opinions extrêmement antidémocratiques ne relèvent pas de la protection de l'article 10 de la CEDH. Toutefois, la Cour a appliqué le test de l'article 10 même pour ces expressions extrêmes dans la presque totalité des situations qu'elle a eue à connaître.

Pour justifier une ingérence au titre de l'article 10 de la CEDH (ou, en d'autres termes, pour éviter la violation du droit protégé par l'article 10), trois conditions doivent être remplies. Premièrement, il doit y avoir une base légale suffisante en droit interne pour la mesure pertinente (« prévue par la loi »). Deuxièmement, cette base légale et les mesures particulières doivent poursuivre des buts nécessaires dans une société démocratique, tels qu'énumérés à l'article 10 section 2 de la CEDH (à savoir la sécurité nationale, la santé publique ou la morale, la protection de la réputation ou des droits de tiers, la protection de la confidentialité). Troisièmement, cette base légale en droit interne et les mesures particulières reposant sur cette base légale doivent être proportionnées.

Dans l'analyse ci-dessous, nous allons faire la différence entre le blocage de contenus par un FSI (fournisseur de services sur internet ou d'accès à internet) et le retrait de contenus par un hébergeur (fournisseurs de services d'hébergement; voir également ci-dessus 1). Le blocage est une mesure qui va très loin et, du point de vue des droits de l'homme, les États devraient être très prudents avant d'y recourir. Dans la perspective des droits de l'homme, un raisonnement légèrement différent s'applique aux mesures prises à l'encontre d'un hébergeur en vue de retirer des contenus en ligne (voir sur ce point plus de détails ci-après, 2.2.1).

2.1. Blocage et filtrage par des FSI

2.1.1. Problématique

Avant d'entrer dans le vif du sujet, il est important de faire référence aux conclusions du **Rapport de l'OSCE sur La liberté d'expression sur internet, études des dispositions pratiques juridiques liées à la liberté d'expression, à la libre circulation de l'information et au pluralisme des médias sur internet (2011)**^{1, 2}.

Pour ce qui est des droits de l'homme, le rapport de l'OSCE identifie trois problèmes.

(1) Le premier est le blocage volontaire, en d'autres termes le blocage est réalisé par le fournisseur de services internet soit entièrement de sa propre initiative, soit sur incitation par les autorités ou gouvernements (voir plus haut, 1.1)³.

« Il est préoccupant que les mécanismes et accords relatifs au blocage volontaire ne respectent pas les principes du procès équitable dans les États qui les appliquent. En l'absence de base légale pour le blocage de l'accès à des sites web, des plateformes et des contenus en ligne, il est possible de s'interroger sur la compatibilité de ces accords et systèmes avec l'article 10 de la Convention européenne des droits de l'homme. Bien que l'on puisse comprendre les bonnes intentions des autorités qui veulent combattre la pédopornographie et d'autres types de contenus illégaux, en l'absence d'une base légale valide en droit interne pour bloquer l'accès à des sites web, l'autorité ou le pouvoir de blocage, d'administration et de conservation des listes noires conféré à certaines organisations et institutions demeure problématique. Une telle « ingérence volontaire » constituera une violation de l'article 10 sauf si les exigences de l'article 10(2) sont remplies et que la nécessité de l'ingérence est établie de manière convaincante. La Cour européenne des droits de l'homme a répété que la liberté d'expression est importante car elle constitue l'une des conditions préalables à une démocratie qui fonctionne bien. Pour l'exercice véritable, « effectif », de cette liberté, l'obligation de l'État de ne pas s'ingérer peut ne pas suffire et doit nécessiter des mesures positives de protection de cette liberté fondamentale. En conséquence, un système de blocage reposant exclusivement sur l'autorégulation ou des « accords volontaires » risque de s'apparenter à une interférence non légitime avec les droits fondamentaux. »⁴ (traduction libre)

(2) Le deuxième concerne le test de l'Article 10 concernant la proportionnalité et la poursuite d'un but légitime :

« Il est rappelé que les cours de justice sont les garantes de la justice et qu'elles ont un rôle fondamental à jouer dans un État régi par la prééminence du droit. En l'absence de base légale valide, le pouvoir de rendre des ordonnances et décisions de blocage accordé à des institutions publiques ou privées autres que les cours de justice pose donc par essence problème du point de vue des droits de l'homme. A supposer même qu'il existe une base légale pour le blocage de sites web, toute ingérence doit être proportionnée au but légitime poursuivi. Dans ce contexte, il est postulé que le blocage basé sur le domaine de sites web et plateformes en ligne contenant des contenus légitimes tels que YouTube, Facebook, Wordpress et Twitter pourrait être incompatible avec l'article 10 et considéré comme une violation grave de la liberté d'expression. Une mesure aussi disproportionnée irait bien plus loin que ce qui est raisonnablement nécessaire dans une société démocratique. Internet joue maintenant un rôle essentiel en tant que moyen de communication de masse, en particulier par le développement de plateformes de type web 2.0 qui permettent aux citoyens de participer activement au débat et au discours politiques. Ces plateformes sont dans le monde entier un vecteur populaire où peuvent s'exprimer des points de vue alternatifs et dissidents. Interdire l'accès à des plateformes de médias sociaux tout entières a donc des implications très fortes pour l'expression politique et sociale⁵. » (traduction libre)

(3) Le troisième concerne les effets d'une restriction préalable, de la censure et des effets dissuasifs :

« Les politiques de blocage au niveau étatique ont sans aucun doute un impact très fort sur la liberté d'expression qui est l'un des principes fondateurs de la démocratie. Les ordonnances de blocage qui sont délivrées et exécutées sans limitation de durée sur des sites web pourraient aboutir à une censure préalable à la publication (« prior restraint »). Bien que la Cour européenne des droits de l'homme n'interdise pas la censure préalable à

1. OSCE, Organisation pour la sécurité et la coopération en Europe, Bureau du Représentant pour la liberté des médias, *REPORT Freedom of Expression on the internet, Study of legal provisions and practices related to freedom of expression, the free flow of information and media pluralism on the internet in OSCE participating states*, 15 décembre 2011, voir en particulier les parties sur le blocage, rapports pays pour les pays membres de l'OSCE : <http://www.osce.org/fom/80723?download=true>.

2. Pour d'autres sources sur le blocage, voir Sieber/Nolde, *Sperrverfügungen im Internet, Nationale Rechtsdurchsetzung im globalen Cyberspace?* (Schriftenreihe des Max-Planck-Instituts für ausländisches und int. Strafrecht, 2008). Messerschmidt, *Internetsperren und Menschenrechte*, http://publikationen.collaboratory.at/mri/internetsperren-und-menschenrechte/#_ftn26. Une publication pourrait être sortie très bientôt par Messerschmidt (thèse à l'Université de Vienne, publiable en 2016). Les conclusions de cette thèse n'étaient pas disponibles au moment de l'étude par le SICL.

3. Les exemples les plus nets sont le Royaume-Uni, les Pays-Bas, le Danemark, la Suède, la Norvège, la Suisse et le Liechtenstein, voir rapport de l'OSCE, p. 145 and 150-169.

4. Rapport OSCE, p. 178, sans références.

5. Rapport OSCE, p. 178, sans références.

la publication, cette solution comporte de tels dangers inhérents qu'elle appelle de la part des tribunaux une analyse particulièrement approfondie de la situation. Ceci est particulièrement vrai pour la presse, les actualités se périssant rapidement, si on retarde une publication, même pour une courte durée, elles risquent de n'avoir plus aucune valeur ou intérêt. Cela vaut aussi pour les nouveaux médias et les publications sur le net. Certains font valoir que la censure préalable à la parution et autres interdictions imposées sur la future publication de journaux entiers, et si l'on va par-là à des sites web et contenus en lignes, sont incompatibles avec les droits consacrés par la Convention européenne des droits de l'homme. La Cour de Strasbourg exige que l'on envisage des mesures moins draconiennes telles que la confiscation de numéros particuliers de publications, y compris des journaux, ou des restrictions à la publication d'articles spécifiques. On est fondé à penser que la pratique consistant à interdire des sites web entiers et la future publication des articles qui s'y trouvent (dont le contenu est inconnu au moment du blocage de l'accès) va au-delà de toute notion de limitation « nécessaire » dans une société démocratique et s'apparente dès lors à de la censure⁶. » (traduction libre).

Ces catégories et problèmes serviront de base à l'analyse ci-après de la position des droits de l'homme dans le contexte du blocage et du retrait de contenus en ligne. Au vu des travaux déjà menés et synthétisés dans le rapport de l'OSCE, l'analyse se concentrera sur les récents développements.

En ce qui concerne la question de la censure préalable à la parution (problématique 3 ci-dessus), très peu de nouveautés sont intervenues. Les principaux problèmes continuent de se poser en ce qui concerne la question de la base légale (problématique 1 ci-dessus) et certaines évolutions se sont produites en matière de proportionnalité avec des objectifs légitimes (problématique 2 ci-dessus). Cette synthèse sera formulée par référence expresse aux différentes sources (Cour européenne des droits de l'homme, documents du Conseil de l'Europe, droit de l'UE).

2.1.2. Les exigences relatives à l'existence d'une base légale pour le blocage et la Cour européenne des droits de l'homme

2.1.2.1. Arrêt *Yildirim* de la Cour européenne des droits de l'homme (2012) : la nécessité claire de disposer d'une base légale

La nécessité de disposer d'une base légale pour toute mesure de blocage (déjà indiquée plus haut) a été analysée plus avant dans l'arrêt de chambre de la Cour européenne des droits de l'homme dans l'affaire *Ahmet Yildirim c. Turquie* (18.12.2012⁷). Dans cette affaire, le blocage de l'accès au site web du requérant avait été déclenché par une ordonnance du tribunal pénal de Denizli dans le cadre d'une procédure pénale à l'encontre du propriétaire d'un autre site qui était accusé d'avoir insulté la mémoire d'Atatürk. Le tribunal avait à l'origine ordonné le blocage de ce seul site. Toutefois, l'autorité administrative responsable de l'exécution de l'ordonnance (le TIB) avait demandé une ordonnance judiciaire pour le blocage de tous les accès à Google Sites qui hébergeait non seulement le site litigieux mais aussi le site du requérant. Le tribunal avait fait droit à la requête, concluant que la seule manière de bloquer le site en question était d'empêcher l'accès à Google Sites tout entier. Bien que ni Google Sites ni le site de M. Yildirim n'aient été concernés par les procédures susmentionnées, le TIB avait rendu l'accès à ces sites techniquement impossible, afin d'exécuter les mesures ordonnées par le tribunal pénal de Denizli.

La Cour a reconnu qu'il ne s'agissait pas là d'une interdiction générale mais plutôt d'une restriction à l'accès à internet. Toutefois, l'effet limité de la restriction ne réduisait pas pour autant sa portée, en particulier du fait qu'internet était à ce moment devenu l'un des principaux moyens d'exercer le droit à la liberté d'expression et d'information. La mesure en question s'apparentait donc à une ingérence par les pouvoirs publics dans le droit du requérant à la liberté d'expression. Cette ingérence violerait l'article 10 à moins d'être prévue par la loi, de poursuivre un ou plusieurs buts légitimes et d'être nécessaire dans une société démocratique pour atteindre ces buts.

L'application d'une règle est « prévisible » si la règle a été formulée avec une précision suffisante pour permettre à quiconque – si nécessaire avec un conseil approprié – de s'y référer pour adapter son comportement. En vertu de la loi n° 5651, un tribunal pouvait ordonner le blocage de l'accès au contenu publié sur internet s'il y avait des raisons suffisantes de suspecter que ledit contenu avait donné lieu à un délit pénal. Toutefois, ni Google Sites ni le site de M. Yildirim n'avaient fait l'objet de procédures judiciaires dans cette affaire. Bien que la décision du 24 juin 2009 ait conclu que Google Sites était responsable du site qu'il hébergeait, aucune disposition ne figurait dans la loi n° 5651 permettant le blocage complet de l'accès tel qu'il avait été ordonné par le tribunal.

6. Rapport OSCE, p. 179 and 25, sans références.

7. Requête n° 3111/10.

La loi n'autorisait pas non plus le blocage d'un domaine internet entier tel que Google Sites. De plus, il n'y avait pas de preuve que Google Sites avait été informé qu'il hébergeait des contenus réputés être illégaux ou qu'il avait refusé d'appliquer une mesure intérimaire concernant un site faisant l'objet de procédures pénales en cours. La Cour a relevé que la loi avait conféré des pouvoirs de grande portée à un organe administratif, le TIB, dans la mise en œuvre d'une ordonnance de blocage délivrée à l'origine en lien avec un site spécifié. Les faits en l'espèce montraient qu'il avait été facile au TIB de demander l'extension de la portée au départ limitée de l'ordonnance de blocage.

La Cour a rappelé qu'une mesure de censure préalable n'est compatible avec la Convention que si un cadre légal strict est en place règlementant la portée d'une interdiction et garantissant la possibilité d'une revue judiciaire pour prévenir de possibles abus. Or, lorsque le tribunal pénal de Denizli avait décidé de bloquer tous les accès à Google Sites, il s'était simplement référé à un avis du TIB sans vérifier si une mesure de portée moindre aurait pu être prise pour bloquer l'accès spécifiquement au site en question. La Cour européenne a en outre observé que rien ne prouvait que le tribunal pénal ait tenté de quelque manière que ce soit de pondérer les divers intérêts en jeu, en particulier en évaluant s'il était nécessaire de bloquer tous les accès à Google Sites. Du point de vue de la Cour, cette lacune était une conséquence du droit interne turc qui ne posait pas d'obligation pour les tribunaux d'examiner si le blocage intégral de Google Sites était justifié. Les tribunaux auraient dû prendre en compte le fait qu'une telle mesure rendrait inaccessibles des volumes importants d'informations, affectant ainsi directement les droits des utilisateurs d'internet et ayant un effet collatéral significatif.

L'ingérence résultant de l'application de l'article 8 de la loi n° 5651 n'avait donc pas respecté l'exigence de prévisibilité consacrée par la Convention et n'avait pas donné au requérant le degré de protection auquel il avait droit du fait de la prééminence du droit dans une société démocratique. La Cour avait également relevé que l'article 10 alinéa 1 de la Convention déclare que le droit à la liberté d'expression s'applique « sans considération de frontières ».

Les effets de la mesure en question avaient donc été **arbitraires** et la **révision judiciaire** du blocage de l'accès avait été insuffisante pour prévenir des abus. La Cour a donc conclu à l'existence d'une violation de l'article 10 de la Convention.

2.1.2.2. L'arrêt *Cengiz de la Cour européenne des droits de l'homme (2015) : la qualité des dispositions légales*

Pour les États qui ont élargi leur base légale existante en matière de blocage (voir ci-après, 2.1.4.2. et ci-dessus, 1.2.1), le problème actuel semble être celui de savoir jusqu'où le système juridique peut aller en ce qui concerne les mesures de blocage, en particulier pour la délimitation des infractions pénales pour lesquelles le blocage peut être ordonné et/ou exécuté. Cette question (problématique 2 ci-dessus : proportionnalité par rapport aux buts légitimes) pourrait avoir été traitée dans l'affaire *Cengiz et autres c. Turquie*⁸ (1.12.2015).

L'affaire concernait le blocage de l'accès à YouTube, un site web permettant aux utilisateurs d'envoyer, de regarder et de partager des vidéos. La Cour européenne des droits de l'homme a conclu en particulier que les requérants, tous universitaires dans différentes universités, avaient été empêchés d'accéder à YouTube pendant une longue période et que, en tant qu'utilisateurs actifs, et compte tenu des circonstances de l'affaire, ils pouvaient légitimement invoquer le fait que l'ordonnance de blocage en question avait affecté leur droit de recevoir et de partager des informations et des idées. La Cour a également observé que YouTube est une plate-forme unique qui permet de diffuser des informations présentant un intérêt spécifique, en particulier sur des questions politiques et sociales, et au journalisme citoyen d'émerger.

La Cour a relevé que l'ordonnance de blocage avait été imposée au titre de l'article 8 (1) de la loi turque n° 5651. La Cour a répété sur ce point que, dans son arrêt dans l'affaire *Ahmet Yildirim contre Turquie*, elle avait déjà conclu que la loi n° 5651 n'autorisait pas le blocage de l'accès à un site internet entier (blocage excessif) du fait de l'un de ses contenus. En vertu de l'article 8 (1), une ordonnance de blocage ne pouvait être imposée à l'égard d'une publication spécifique que s'il y avait des motifs de soupçonner un délit. Il ressortait donc que dans l'affaire en question, il n'y avait pas eu de législation permettant au tribunal pénal de première instance d'Ankara d'imposer une ordonnance de blocage général à l'accès à YouTube. La Cour a en conséquence conclu que l'ingérence n'avait pas satisfait à la condition de légitimité requise par la Convention et que M. Cengiz, M. Akdeniz et M. Altiparmak n'avaient pas bénéficié d'un degré suffisant de protection. Sur la base de ce raisonnement, il n'y avait ni urgence ni nécessité que la Cour donne de plus amples explications.

Dans l'intervalle, toutefois, le législateur turc avait élargi la base légale pour le blocage. Cette nouvelle législation n'était pas applicable dans l'affaire *Cengiz*; elle constitue une base légale pour le blocage excessif. La

8. Requêtes n° 48226/10 et 14027/11.

Cour n'a pas directement traité le problème. Toutefois, le juge Lemmens a évoqué une occasion manquée dans son opinion dissidente :

« Après avoir conclu que l'ingérence litigieuse ne répondait pas à la condition de légalité posée par le paragraphe 2 de l'article 10 de la Convention, la majorité a estimé qu'il n'était pas nécessaire de contrôler le respect des autres exigences de ce paragraphe (paragraphe 67 de l'arrêt). En principe, une telle approche se justifie. Toutefois, dans les circonstances de la présente affaire, je pense qu'il s'agit d'une occasion manquée.

En effet, la disposition légale sur laquelle la Cour s'est prononcée, à savoir l'article 8 de la loi n° 5651, a entre-temps été complétée par une disposition, l'article 8A, qui prévoit désormais expressément que l'accès à l'intégralité d'un site internet peut être bloqué (paragraphe 22 de l'arrêt). Le présent arrêt porte donc sur une situation qui, pour autant qu'elle concerne la base légale de la mesure incriminée, appartient largement au passé. Dans ces circonstances, il aurait été souhaitable, à mon avis, d'examiner si, indépendamment du fait que l'ingérence litigieuse n'était pas prévue par la loi, cette mesure poursuivait un but légitime et si, eu égard notamment à ses effets, elle était proportionnée à ce but (voir, pour une approche similaire, *Kurić et autres c. Slovénie* [GC], n° 26828/06, § 350, CEDH 2012).

Certes, la Cour ne doit pas se prononcer *in abstracto* sur le nouvel article 8A (paragraphe 75 de l'arrêt). J'estime néanmoins que, si elle avait examiné, fût-ce par *obiter dictum*, la finalité et la nécessité de l'ingérence litigieuse, son arrêt aurait pu éclairer les citoyens et les autorités turcs sur les principes auxquels doivent répondre tant les applications de l'article 8 que celles du nouvel article 8A de la loi n° 5651. »

A la date de rédaction de cette présente étude (mi-décembre 2015), on ne sait pas clairement si cette affaire sera examinée par la Grande chambre de la Cour européenne des droits de l'homme.

La question de la légitimité, de la nécessité et de la proportionnalité tend à prendre de plus en plus d'importance dans les juridictions qui se sont dotées d'une législation spécifique, en cours d'expansion et d'élargissement. De nombreux États commencent à peine à adopter une législation à cet égard. C'est pourquoi il est très important que le test de l'article 10, pour ce qui est de la qualité des dispositions législatives, soit appliqué dans une affaire concernant spécifiquement le blocage de contenus.

Le principal obstacle à surmonter pour ces mesures législatives en expansion sera celui de leur nécessité dans une société démocratique pour atteindre des buts légitimes. L'un de ces buts peut être la **protection de la réputation individuelle**. La principale question non encore résolue est le fait de savoir si les lignes directrices dégagées sur cette question dans les affaires hors ligne (médiat imprimés) peuvent aussi s'appliquer à des affaires en ligne, ou si la Cour tiendra compte du danger spécial créé par les publications sur internet et permettra donc que soient appliquées aux contenus en ligne des restrictions plus larges que celles qu'elle autoriserait pour la presse écrite. Cette dernière approche semble recueillir un certain soutien⁹. Que la Cour suive ou non les mêmes lignes directrices, il convient de garder à l'esprit que les personnes qui contribuent à animer le débat public doivent faire face à plus de critiques que les autres, que ce soit en ligne ou hors ligne¹⁰.

2.1.3. Base juridique et blocage volontaire et le Conseil de l'Europe

Le danger d'un blocage ou d'une suppression volontaire d'informations par des acteurs privés est préoccupant pour le Conseil de l'Europe. À cet égard, le **Comité des Ministres** a formulé des recommandations en 2011¹¹ :

« [L]es compagnies concernées ne sont pas à l'abri d'une ingérence abusive ; leurs décisions découlent parfois de pressions politiques directes ou de contraintes économiques à motivation politique, en invoquant une justification basée sur le respect de leurs modalités de service.

5. Ces évolutions montrent que la libre parole sur l'internet fait face à de nouveaux défis et qu'elle pourrait être victime **des mesures prises par des plateformes internet gérées par des exploitants privés et des prestataires de services en ligne**. Il est donc nécessaire de reconnaître le rôle de ces acteurs en tant que facilitateurs de l'exercice de la liberté d'expression et du droit à la liberté de réunion et d'association.

6. Les ingérences dans les contenus diffusés dans le **domaine public** par l'intermédiaire de ces moyens ou les tentatives visant à **rendre inaccessibles des sites internet entiers** devraient être examinées au regard des

9. Voir Grabenwarter, *Commentaires CEDH*, 2014, article 10, n° 59 : « Le risque de préjudice que le contenu et les communications sur internet font peser sur l'exercice et la jouissance des droits de l'homme et des libertés fondamentales, en particulier le droit au respect de la vie privée, est sans aucun doute supérieur à la menace que constitue la presse. La Cour conclut donc que les politiques régissant la reproduction de contenu tiré de la presse écrite et tiré d'internet peuvent être différentes. Les journalistes doivent être en mesure d'utiliser les informations tirées d'internet sans craindre d'être sanctionnés. » (renvoie à la Cour, 5 mai 2011, *Editorial Board of Pravoye Delo and Shtetel versus Ukraine*, N°. 33014/05, § 63). Cette affaire ne concernait cependant que la reproduction de contenu illégal et non le blocage en tant que tel.

10. Benedek/Kettemann, *Freedom of Expression and the internet*, 2013, p. 91 : sur le « *libel tourism* ». Les États « doivent appliquer les garanties de protection de la liberté d'expression hors ligne à des situations en ligne, même s'il faut élaborer ces garanties en reconnaissant l'impact spécial qu'ont souvent les publications sur internet ».

11. Déclaration du Comité des Ministres sur la protection de la liberté d'expression et de la liberté de réunion et d'association en ce qui concerne les plateformes internet gérées par des exploitants privés et les prestataires de services en ligne, adoptée par le Comité des Ministres le 7 décembre 2011, à la 1129^e réunion des Délégués des Ministres.

normes internationales de protection de la liberté d'expression et du droit de communiquer et de recevoir des informations, notamment les dispositions de l'article 10 de la Convention et la jurisprudence correspondante de la Cour européenne des droits de l'homme. De plus, les obstacles à l'interaction de certaines communautés d'intérêt spécifique devraient également être examinés au regard des normes internationales relatives au droit à la liberté de réunion et d'association, en particulier les dispositions de l'article 11 de la Convention et la jurisprudence correspondante de la Cour européenne des droits de l'homme.»

De plus, le Commissaire aux droits de l'homme du Conseil de l'Europe a publié un document thématique en 2014 sur la prééminence du droit sur internet et dans le monde numérique¹². Ce document, qui traite du blocage volontaire au Royaume-Uni et en Suède, précise ce qui suit¹³:

« Il est réellement permis de douter qu'un système de blocage qui impose effectivement une restriction à l'accès des personnes ordinaires aux informations en ligne soit jamais conforme à la prééminence du droit, lorsqu'il est choisi par des parties privées qui l'utilisent, sans surveillance du public, sans débat démocratique, sans cadre juridique prévisible, sans objectif et cible clair, sans preuve de son efficacité, de sa nécessité et de sa proportionnalité, et sans évaluation ex ante ou ex post de ses effets potentiellement contreproductifs [traduction libre].

Si toutes les considérations touchant à l'efficacité et à la proportionnalité de la mesure restent pertinentes, ce type de blocage soulève une question plus générale et plus fondamentale qui appelle une réponse: dans quelle mesure ces décisions de blocage sont-elles vraiment volontaires et/ou engagent-elles la responsabilité de l'État? Si, s'agissant de ce droit, l'article 10 de la CEDH ne mentionne que les ingérences « d'autorités publiques », cela ne signifie pas que l'État peut, purement et simplement, décliner toute responsabilité vis-à-vis de mesures d'entités privées produisant cet effet, et ce d'autant moins s'il encourage vivement ces mesures *de facto*. Dans ces circonstances, il est responsable de ne pas avoir donné à un tel système une base législative: sans cette base, les restrictions ne sont pas prévues par la loi » [traduction libre].

Bon nombre de ces mesures de blocage sont contenues dans des mécanismes d'autorégulation et dans les termes des contrats des FSI. La recommandation du **Comité des Ministres** sur la libre circulation transfrontière des informations sur internet, du 1^{er} avril 2015, rappelle aux FSI que cette autorégulation doit respecter les normes des droits de l'homme:

« Les États devraient encourager, faciliter et soutenir l'élaboration de **codes d'autorégulation appropriés**, de façon à ce que tous les acteurs respectent le droit à la vie privée et familiale, le droit à la liberté d'expression et le droit à la liberté de réunion et d'association, dans le plein respect des articles 8, 10 et 11 de la CEDH, notamment en ce qui concerne la libre circulation du trafic internet¹⁴. »

2.1.4. Développements dans l'UE concernant la base légale et le blocage volontaire

2.1.4.1. Cas spécial: violations des droits d'auteur, CJE et juridictions nationales

Dans le domaine de la protection des droits d'auteur, la législation de l'UE a inscrit un article 8 alinéa 3 de la Directive sur la société de l'information¹⁵, en vertu duquel un FSI peut être considéré comme une sorte de co-auteur « passif » en cas de **violation des droits d'auteur**¹⁶. Ceci affecte un groupe relativement large de pays, à savoir les États membres de l'UE. Tous ceux-ci ont depuis transposé cette disposition en droit interne. En 2014, la Cour européenne de justice a décidé dans sa décision *UPC Telekabel Wien*¹⁷ (connue également comme l'affaire « *kino.to* », dans une conclusion préliminaire sur saisine d'un tribunal autrichien) que le détenteur d'un droit d'auteur peut invoquer la Directive sur la société de l'information pour obtenir une ordonnance à l'encontre d'un FSI. La Cour européenne de justice a mené une évaluation très approfondie et conséquente des droits de l'homme dans cette affaire, prenant en compte toutes les personnes intéressées, les perspectives et plusieurs autres droits de l'homme. Il y a donc une base légale pour les mesures de blocage pour les États concernés dans ce domaine.

12. CommDH/IssuePaper(2014)1 du 08 décembre 2014, consultable: http://www.coe.int/t/dghl/standard_setting/media/cdmsi/Rule_of_Law_internet_Digital_World.pdf

13. Ibid, p. 72 et seq.

14. Recommandation CM/Rec(2015)6 du Comité des Ministres aux États membres sur la libre circulation transfrontière des informations sur internet, adoptée par le Comité des Ministres le 1^{er} avril 2015 à la 1224^e réunion des Délégués des Ministres, point 3 Valeur de l'autorégulation.

15. Directive 2001/29/CE du Parlement européen et du Conseil du 22 mai 2001 relative à l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information.

16. L'article 8 alinéa 3 dispose ceci: « Les États membres veillent à ce que les titulaires de droits puissent demander qu'une ordonnance sur requête soit rendue à l'encontre des intermédiaires dont les services sont utilisés par un tiers pour porter atteinte à un droit d'auteur ou à un droit voisin. »

17. C-314/12 – UPC Telekabel Wien. Arrêt de la Cour (Quatrième chambre) du 27 mars 2014. *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH*.

Des jugements nationaux sur cette base ont suivi et d'autres viendront encore. Pour bon nombre des systèmes juridiques nationaux qui sont déjà dotés d'une législation sur le blocage, cette décision n'a pas changé grand-chose puisque leurs dispositions législatives mentionnaient déjà les violations aux droits d'auteur. Pour les systèmes nationaux (comme celui de l'Autriche ou de l'Allemagne, par exemple) qui n'avaient pas du tout reconnu les mesures de blocage, ce tournant a été difficile à prendre et il a fallu actionner des sources de droit national qui n'étaient pas vraiment adaptées à cette fin. Ainsi, en Autriche, la Cour suprême a fait de son mieux pour intégrer ces mesures sur la base d'un «*Erfolgsverbot*» dans le cadre de la loi sur les recours civils¹⁸. Des doutes subsistent, mais les tribunaux autrichiens ont refusé de demander une fois encore l'avis de la Cour de justice européenne ou de tester la compatibilité de leurs solutions par rapport à la Constitution fédérale autrichienne. En Allemagne, la Cour fédérale a décidé très récemment de recourir à la notion de «*Störerhaftung* (responsabilité de l'auteur d'une perturbation)» comme base pour les ordonnances de blocage. Dans le même temps, elle a décidé que le blocage doit être subsidiaire aux autres mesures de protection. De sorte que, pour obtenir une ordonnance de blocage, un plaignant doit d'abord démontrer les mesures qu'il a déjà prises pour tenter d'obtenir le retrait des contenus visés¹⁹.

De très vives objections ont aussi été formulées à l'égard de cette évolution introduite par la Cour européenne de justice; en particulier, les juridictions inférieures allemandes ont refusé de suivre l'orientation de cette dernière du fait de l'efficacité limitée des mesures de blocage qui pourraient constituer un problème sur le plan des droits de l'homme en termes de **proportionnalité** et de transfert de compétence judiciaire aux fournisseurs d'accès²⁰ et de services sur internet. Même dans ce domaine des violations des droits d'auteur, nous n'avons vraisemblablement pas encore vu la fin de l'histoire²¹.

Étant donné que le blocage n'est **pas très efficace** en général, les États ont déjà commencé à trouver des solutions nouvelles, en particulier dans le domaine du droit d'auteur. Une sorte de blocage de nouvelle génération pour des violations des droits d'auteur, par exemple, a été utilisée en France, est actuellement l'objet de litiges en Irlande et va bientôt apparaître probablement dans la législation de bon nombre d'autres pays. Selon cette approche, les détenteurs de droits d'auteur non seulement s'appuient sur les ordonnances classiques de blocage, mais tentent aussi de forcer les FSJ à «bloquer» (du moins à obtenir le paiement de redevances) ceux de leurs clients qui téléchargent des contenus protégés sans versement de droit. Un client a droit à «trois tentatives» puis «il est bloqué» (ou alors il s'acquitte de redevances pour le téléchargement en faveur du détenteur des droits). Étant donné que ceci aboutit à une exclusion de l'accès à internet, cette approche pose bien entendu un problème à un autre niveau, à savoir l'accès à internet en tant que droit de l'homme. Une telle «interruption» de l'accès par des internautes en situation de violation est soumise au test de l'article 10. Des recours procéduraux doivent être en place et l'interruption ne peut intervenir que pour une période très limitée²². Ainsi, dès que les redevances sont versées ou que l'utilisateur atteste dans une déclaration qu'il ne commettra pas d'autres violations, l'accès à internet doit être rétabli.

2.1.4.2. L'UE et le blocage dans d'autres domaines

Dans toutes les autres branches du droit, l'UE est restée passive en ce qui concerne le blocage. Certaines tentatives ont été faites pour élaborer des règles de blocage en vue de lutter contre le **terrorisme** et la **pédopornographie**, mais elles n'ont pas produit de résultats contraignants pour les États membres²³.

18. Voir la contribution nationale de l'Autriche à cette étude, point 2.1. Voir aussi Angelopoulos, *Les ordonnances de blocage contre des FSJ sont-elles autorisées en Europe? Application contraignante des droits d'auteur dans le paysage juridique de Post-Telekabel*, in *GRUR Int.* 2014, 1089: «Les effets véritablement négatifs de la décision devraient vraisemblablement être limités à l'Autriche – la plupart des États membres n'ont pas de mécanisme procédural comparable à l'*Erfolgsverbot*. A titre indicatif, la question a déjà été examinée l'an dernier par le juge britannique Arnold dans l'affaire *EMI Records v. British Sky Broadcasting*, qui a conclu que puisqu'en vertu du droit du Royaume-Uni, les tribunaux doivent prendre soigneusement compte les **droits fondamentaux** et la proportionnalité avant de délivrer une ordonnance de blocage, la question ne s'applique pas aux tribunaux du Royaume-Uni».

19. BGH, 26.11.2015, I ZR 3/14; I ZR 174/14. Voir Becklink 2001774. A cette date (mi-décembre 2015), le jugement n'a pas encore été publié.

20. Nazari-Khanachayi, *Access-Provider als urheberrechtliche Schnittstelle im Internet*, *GRUR* 2015, 115, 120: „Gerade weil der EuGH die rechtsstaatlichen Anforderungen vollständig außer Acht gelassen hat, darf erwartet werden, dass betroffene Internetnutzer und/oder Access-Provider im Falle einer unbestimmten Anordnung den Gang zu den nationalen Instanzengerichten riskieren werden, um eine Vorlagefrage im Hinblick auf die Zulässigkeit der herbeigeführten Übertragung von (faktischen) Hoheitsbefugnissen auf einen privaten Marktakteur zu erwirken“.

21. Voir Husovec/Peguera: *Much Ado about Little – Privately Litigated Internet Disconnection Injunctions*, in *IIC* 2015, 10: «Ces ordonnances posent de sérieux problèmes pour ce qui concerne leur compatibilité avec la Charte des droits fondamentaux de l'UE. En effet, la possibilité que des ordonnances efficaces de cette nature se conforment en même temps aux droits de l'homme devient très étroite. En d'autres termes, les dispositions de la Directive sont très prometteuses mais, si elles sont appliquées correctement, ne donnent que peu de résultats.» (traduction libre).

22. Voir Benedek/Kettemann, *Freedom of Expression and the Internet*, p. 75 et suivantes.

23. Voir le Rapport OSCE, p. 139 et suivantes. Pour les activités de l'UE dans le domaine de la liberté d'expression, voir Benedek/Kettemann, *Freedom of Expression and the Internet*, p., 152.

Le droit de l'UE stipule bien qu'il y a un privilège d'exonération de responsabilité pour les FSI dans la **Directive sur le commerce électronique**²⁴. Les FSI ne peuvent pas voir leur responsabilité engagée au civil ou au pénal pour avoir juste transféré passivement des informations, même s'ils ont été notifiés auparavant²⁵. Ils ne peuvent pas non plus être obligés à surveiller les contenus. Cela n'empêche pas cependant un tribunal ou une autorité administrative d'exiger du fournisseur de services qu'il mette fin à une violation ou qu'il prenne des mesures préventives, conformément aux systèmes juridiques d'un État membre (autrement dit, si le droit interne le prévoit spécifiquement). On peut penser qu'une législation spécifique prévoyant des mesures de blocage est requise. Bon nombre d'États membres n'ont pas reconnu ce besoin au moment de la publication de la Directive sur le commerce électronique (2001) et ont souhaité baser les ordonnances de blocage à l'encontre de FSI sur la simple illégalité du contenu²⁶.

La **Commission européenne** envisage à l'heure actuelle de modifier la Directive sur le commerce électronique sur ce point (**Stratégie pour un marché numérique unique**²⁷). Ceci pourrait passer par une obligation de diligence pour tous les fournisseurs de services²⁸. Toutefois, il est plutôt improbable que ceci aboutisse à une obligation positive des FSI de bloquer les contenus. Il semble plus probable que la législation sur le blocage au niveau du droit interne sera plus importante à cet égard. Et l'UE a déjà pris certaines mesures concernant le blocage.

2.1.4.3. Le Règlement de 2015 sur l'accès à un internet ouvert

Pratiquement vers la fin de la période prévue pour la préparation de l'étude actuelle (fin novembre 2015), l'UE a adopté son **Règlement sur l'accès à un internet ouvert**²⁹. Cet instrument contient (de manière légèrement cachée) des dispositions pertinentes pour le blocage³⁰. Il consacre la doctrine de la non-surveillance telle qu'elle figurait dans la Directive sur le commerce électronique³¹. Les nouvelles dispositions entreront en vigueur le 30 avril 2016. L'approche de base est que **tout blocage du contenu est explicitement interdit**, sauf pour les exceptions (plus ou moins) étroites prévues dans le texte³². Le premier point important à mentionner ici est que le simple blocage volontaire sans base légale (en particulier le blocage volontaire de contenu juridique par les FSI) sera interdit (article 3, alinéa 3, lettre a du Règlement). Ceci équivaut à **l'interdiction d'un blocage**

24. Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« directive sur le commerce électronique »).

25. Art. 12 E-Com-Dir.

26. Le législateur autrichien voulait « conserver » le blocage basé sur la règle de droit relative à la diffamation dans le Code civil autrichien (voir le contenu législatif tel que cité par Brenn, ECG, 2002, § 19 No. 3, p. 305, 307). Toutefois, pour lui, la règle relative à la diffamation pouvait servir de base à une ordonnance de retrait à l'encontre de l'hébergeur, mais pour une ordonnance de blocage à l'encontre d'un FSI.

27. Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, Stratégie pour un marché unique numérique en Europe, 6.5.2015, COM(2015) 192 final.

28. Ibid, pt. 3.3.2.: Le principe, consacré par la directive sur le commerce électronique, selon lequel les prestataires de services intermédiaires sur l'internet ne doivent pas être tenus pour responsables du contenu qu'ils transmettent, stockent ou hébergent tant qu'ils se cantonnent à un rôle strictement passif a été un pilier du développement de l'internet en Europe. Cela étant, lorsque des contenus illicites sont détectés, qu'il s'agisse d'informations relatives à des activités illégales telles que le terrorisme/la pédopornographie ou d'informations portant atteinte aux droits de propriété d'autrui (par exemple, le droit d'auteur), les intermédiaires devraient prendre les mesures qui s'imposent pour les supprimer. Aujourd'hui, le blocage de l'accès aux contenus illicites et leur retrait par les prestataires de services d'hébergement peuvent s'avérer lents et compliqués, tandis que des contenus bel et bien licites risquent d'être supprimés par erreur. 52,7 % des parties prenantes estiment que les mesures prises pour lutter contre les contenus illicites sont souvent inefficaces et manquent de transparence. Les pratiques nationales divergentes peuvent entraver le contrôle de l'application des règles (et, partant, la répression de la cybercriminalité) et susciter la défiance à l'égard des environnements en ligne. Les pressions qui s'exercent sur le système actuel risquent de s'accroître à mesure que le volume des contenus numériques disponibles sur l'internet augmente. Il n'est pas toujours aisé de circonscrire les droits dont peuvent user les intermédiaires à l'égard du contenu qu'ils transmettent, stockent ou hébergent sans perdre le bénéfice des dérogations en matière de responsabilité prévues par la directive sur le commerce électronique.

Les événements récents sont venus s'immiscer dans le débat public sur l'opportunité de relever le niveau général de protection contre les contenus illicites circulant sur l'internet. Parallèlement à son évaluation des plateformes en ligne, la Commission analysera la nécessité d'élaborer de nouvelles mesures contre les contenus illicites sur l'internet en tenant pleinement compte de leur incidence sur le droit fondamental à la liberté d'expression et d'information, telles que des procédures strictes pour retirer les contenus illicites en épargnant les contenus licites, et elle examinera s'il y a lieu d'imposer aux intermédiaires une obligation de responsabilité et de vigilance accrues dans la gestion de leurs réseaux et systèmes, c'est-à-dire un devoir de diligence.»

29. Règlement (UE) 2015/2120 du Parlement européen et du Conseil du 25 novembre 2015 établissant des mesures relatives à l'accès à un internet ouvert et modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques et le règlement (UE) n° 531/2012 concernant l'itinérance sur les réseaux publics de communications mobiles à l'intérieur de l'Union.

30. Point intéressant, le blocage est réglementé entre la discussion d'un internet à deux classes et l'interdiction de l'itinérance pour les téléphones portables, ce qui est surprenant.

31. Point 10 du Préambule. La Directive sur le commerce électronique reste en fait complètement inchangée.

32. Point 12 du Préambule.

non autorisé par une ordonnance judiciaire et peut **changer fondamentalement l'environnement en matière de blocage**.

Le « mécanisme d'autorégulation » ne peut fonctionner que jusqu'au 31 décembre 2016³³. Après cela, toute activité de blocage devra avoir une base légale sous une forme ou une autre, tel qu'expliqué dans les « exceptions » prévues dans le Règlement.

Le principal environnement pour ces règles sur le blocage est le droit de la concurrence et le droit administratif (autrement dit les relations entre FSI, et entre ces derniers et les autorités nationales). Toutefois, le Règlement lui-même consacre le droit d'accès à un internet ouvert dans tout contrat entre un FSI et ses clients ; les FSI doivent mettre en place des procédures transparentes, simples et efficaces pour traiter les réclamations des utilisateurs finaux en ce qui concerne les droits et obligations consacrés dans l'article 3 (interdiction de blocage). En conséquence, tout client peut porter plainte contre un blocage n'ayant pas une source judiciaire. De plus, **l'autorité nationale de surveillance** compétente a le pouvoir d'examiner les blocages et de poursuivre les violations (article 5 partie 3). Le droit national définira les sanctions applicables pour des violations de l'article 3 (article 6).

Le nouveau Règlement suit une approche plutôt extensive en ce qui concerne les exceptions à l'interdiction du blocage. Contrairement à certains systèmes nationaux, il ne contient pas lui-même une liste de sujets pour lesquels le blocage est admissible mais renvoie essentiellement aux **droits nationaux, à des « mesures » nationales et à « d'autres mesures » basées sur le droit**. Certains documents préparatoires du Parlement européen font référence directement aux droits d'auteur et à l'arrêt *kino.to* de la Cour de justice européenne³⁴.

Le nouveau Règlement non seulement fait référence aux lois et mesures nationales, mais aussi au **droit de l'UE**. L'exigence de conformité avec le droit communautaire s'étend, entre autres, à la conformité avec les exigences de la Charte des droits fondamentaux (CDF) de l'UE pour ce qui concerne les limitations à l'exercice des droits et libertés fondamentaux. Cela signifie que les droits nationaux ou mesures nationales relatifs au blocage doivent être conformes à la Charte des droits fondamentaux. Plus important, toute mesure susceptible de restreindre ces droits et libertés fondamentaux ne peut être imposée que si elle est appropriée, proportionnée et nécessaire dans une société démocratique et que si sa mise en œuvre est soumise à des **sauvegardes procédurales adéquates en conformité avec la Convention européenne des droits de l'homme**, notamment concernant ses dispositions relatives à une protection judiciaire effective et à un procès équitable³⁵.

Il convient de noter que le point 13 du préambule du Règlement mentionne non seulement « des mesures » (telles qu'une ordonnance judiciaire directe à l'encontre d'un FSI) mais aussi « d'autres mesures ». Ceci fait référence à toute mesure garantissant la conformité avec des textes législatifs de l'UE ou avec la législation nationale (par exemple, des obligations de conformité avec des ordonnances judiciaires ou des ordonnances rendues par des pouvoirs publics exigeant le blocage de contenus illégaux). Ceci pourrait impliquer qu'il n'est pas nécessaire d'obtenir concrètement une ordonnance judiciaire ou une décision exigeant chaque acte de blocage ; la simple possibilité qu'une ordonnance judiciaire (ou décision de justice) puisse hypothétiquement être délivrée dans les circonstances semblent être une base suffisante de blocage par un FSI. Cette conclusion est très importante en ce qui concerne les **aspects procéduraux**.

Ce nouveau Règlement impose une sorte de nouveau cadre législatif pour procéder à des blocages au sein de l'UE. Toutefois, la question essentielle de ce qui peut être bloqué, où et quand, demeure à l'évidence très fortement influencée par les **droits nationaux** et les particularités nationales, tel que décrits dans les diverses contributions nationales à la présente étude. Le Règlement ne changera rien à cet égard.

Le principal changement est que certaines juridictions seront confrontées à la nécessité de réactualiser leurs **mécanismes d'autorégulation pour le blocage** (ceci s'applique au Royaume-Uni et à sa fondation *Internet Watch Foundation*, au blocage volontaire danois, suédois et norvégien³⁶ de la pédopornographie et à la base légale plutôt faible en Finlande pour le blocage de la pédopornographie³⁷).

En vertu de la teneur du nouveau Règlement, tout trafic doit être traité de manière équitable, sous réserve d'exceptions strictes et clairement identifiées dans l'intérêt du public, basées sur le droit. L'avenir dans ce domaine pourrait donc se traduire par davantage d'ordonnances de retrait délivrées à l'encontre des fournisseurs de services d'hébergement (voir ci-après, 2.2) et par une coopération internationale accrue pour obtenir des retraits (par exemple INHOPE).

33. Article 10 n° 3

34. Voir EPRS, *The EU rules on network neutrality: key provisions, remaining concerns*, novembre 2015, p. 4, 5 ([http://www.paulruebig.eu/attachments/article/1445/EPRS_BRI\(2015\)571318_EN.pdf](http://www.paulruebig.eu/attachments/article/1445/EPRS_BRI(2015)571318_EN.pdf)); en allemand, avec une référence à *kino.to*: <http://blog.lehofer.at/2015/07/offenes-internet.html>.

35. Pour le tout, voir point 13 du Préambule et Article 3 n° 3 alinéa 3 lit. a.

36. Le nouveau règlement est pertinent pour l'EEE.

37. Voir à cet égard les rapports pays (question 5) pour les pays qui connaissent le blocage volontaire ou privé.

2.1.5. Évaluation

Il y a une jurisprudence considérable et claire de la Cour européenne des droits de l'homme et divers contenus, notamment des recommandations du **Conseil de l'Europe** sur le sujet du blocage et la base judiciaire nécessaire pour de telles mesures. Ces éléments sont soutenus par un certain volume de littérature convaincante³⁸.

2.1.5.1. Blocage sans fondement juridique

Le **blocage sans base légale** est très préoccupant. Au sein de l'**UE**, ce blocage, lorsqu'il existe, ne pourra pas être maintenu après le début de 2017. Les nouvelles règles du droit européen constituent bien une nouvelle étape sur la voie d'un internet ouvert. Même dans des affaires graves, tels que le blocage pour pédopornographie, les FSI ne peuvent pas simplement procéder à un blocage sans base légale spécifique. Les fondements légaux pertinents permettraient une intervention judiciaire pour prévenir les abus. Ceci est d'autant plus important dans les affaires de blocage reposant sur des motifs moins graves.

2.1.5.2. Élargissement de la législation sur le blocage ou adoption de nouvelles dispositions à cet égard

Les États qui disposent déjà de dispositions légales concernant le blocage ont tendance à les élargir et à les étendre, par exemple en Turquie ou en France. Le problème se posera dans les futures affaires en provenance de la Turquie, mais vraisemblablement aussi d'autres États. Ces États restreignent de plus en plus la liberté d'expression par le biais de ces extensions de leur législation.

Il existe aussi de nombreuses **lois nouvelles sur le blocage** dans d'autres États (par exemple, la Suisse a une proposition de blocage des paris illégaux et en cas de violation de droits d'auteur ; en Allemagne, il y a débat sur une législation spécifique pour les droits d'auteur³⁹ et l'Autriche envisage de bloquer les paris étrangers). Dans ces États, cependant, les législations tendent à éviter le **blocage excessif**, autant que possible, et cela pourrait les différencier de la Turquie.

2.1.5.3. Évaluation de la qualité des bases légales et juridiques

D'une part, il est accepté (et salué) que les États basent de plus en plus leur blocage sur des lois spécifiques. Toutefois, il devrait y avoir des limites aux motifs pour lesquels un blocage pourrait être considéré comme nécessaire et justifié. Des expressions vagues telles que « extrémisme » (Russie) ou « propagande » pourrait ne pas être suffisantes pour autoriser le blocage, étant donné que la manière dont ces termes font référence à un objectif légitime spécifique au titre de l'article 10 (2) de la Convention européenne des droits de l'homme pourrait ne pas être claire. Il conviendrait donc de préciser plus explicitement quel type d'extrémisme ou de propagande est visé.

Pour la **Suisse** et le **Liechtenstein**, il convient d'ajouter que certaines dispositions relatives au blocage ne prévoient que des « recommandations » de blocage émises par les autorités à destination des FSI. Cette approche tente de transférer la décision de blocage du secteur public au secteur privé et est confrontée à la même critique que le blocage volontaire (voir ci-après, 2.1.5.4).

Le blocage de sites de **paris** étrangers illégaux est discutable, si un État encourage (où ne prévient pas de manière sérieuse) les offres étendues de paris en ligne par des sociétés nationales ou n'a pas mis en place de mesures particulières de prévention de l'addiction au niveau national. Dans ce cas, un tel blocage pourrait ne pas sembler nécessaire dans une société démocratique donnée. On pourrait suivre le même raisonnement que celui appliqué aux monopoles sur les jeux et paris en général, puisque le blocage en ligne de sites de paris affecte d'abord et avant tout les sites étrangers et ne fait que protéger un système monopolistique de l'État. On peut se référer à la jurisprudence pertinente de la Cour européenne de justice à cet égard.

En résumé de ces réflexions sur la mise en place accrue de bases juridiques spécifiques pour le blocage, on peut se référer à la déclaration du juge Lemmens dans l'affaire récente *Cengiz*, telle que citée plus haut : une évaluation de la qualité des lois pertinentes en matière de blocage est essentielle. La mesure de blocage (prévue en droit) doit être nécessaire dans la société démocratique pour poursuivre un ou plusieurs des buts légitimes énumérés à l'article 10 (2) de la Convention européenne des droits de l'homme et la mesure doit respecter les limites de proportionnalité.

38. A titre d'exemple Akdeniz, *To Block or Not to Block: European Approaches to Content Regulation, and Implications for Freedom of Expression*, in Azevedo Cunha/Gomes De Andrade/Lixinski/Fétaira (eds.), *New Technologies and Human Rights, Challenges to Regulation*, 2013, p. 47, en particulier les conclusions p. 70 et suivantes.

39. Nazari-Khanachayi: *Access-Provider als urheberrechtliche Schnittstelle im Internet* GRUR 2015, 115, 120: l'auteur développe des idées pour de futurs développements. La création d'une base légale serait nécessaire (même s'il part de l'hypothèse que le BGH ne recourrait pas à la responsabilité de l'auteur de la perturbation, ce que ce dernier a fait en définitive), un service d'exécution spécial devrait être mis en place, comme l'IWF au Royaume-Uni et, en attendant que le législateur réagisse, les FSI doivent traiter le problème dans leurs conditions contractuelles standard.

2.1.5.4. Blocage volontaire

Dans l'affaire *Yildirim* (voir plus haut, 2.1.2.1), la Cour européenne des droits de l'homme a déclaré que les restrictions à l'accès à une source d'information n'étaient compatibles avec la Convention que si le pays disposait d'un cadre juridique strict règlementant la portée de l'interdiction et garantissant la possibilité d'une révision judiciaire pour prévenir d'éventuels abus⁴⁰. Toutefois, il semble que même après ces décisions, les États qui encourageaient le **blocage volontaire** ont tout simplement continué leur pratique. Bon nombre d'États estiment que leurs systèmes sont en conformité avec elle (point 5 des contributions nationales) : la critique du droit national dans le pays sur la base de l'affaire *Yildirim* semble peu importante. L'excuse qu'un tel blocage ne pourrait être dirigé que contre des contenus constituant une infraction grave n'est pas convaincante.

L'État ne peut pas s'exonérer de sa responsabilité au motif que le blocage volontaire de contenus (manifestement) illégaux est assuré par des sociétés privées ou par des individus. Certains mécanismes en droit international établissent la responsabilité de l'État pour les violations de droits de l'homme commises par des sociétés privées. Une de ces situations est couverte par la doctrine dite des « entités paraétatiques »⁴¹. Il ne peut pas être exclu que cette doctrine puisse également s'appliquer à la disposition relative à la fourniture d'accès sur internet. Des États (tels que la Suisse, le Lichtenstein avec ses règles et recommandations, ou encore le Royaume-Uni et l'IFW) encouragent en permanence le blocage volontaire sans base légale, et les éventuelles violations de la liberté d'expression par des sociétés privées peuvent être considérées comme des violations commises par l'État lui-même⁴².

Cela étant, un fait ne laisse pas de surprendre : les décisions de la Cour européenne des droits de l'homme ou de tribunaux nationaux relatives au blocage en-dehors du domaine des violations de droits d'auteur et en dehors de la Turquie ne semblent pas trop fréquentes. Cela pourrait s'expliquer par le fait que, dans des systèmes prévoyant le blocage volontaire, il pourrait y avoir un manque de transparence des mesures de blocage, mais aussi que, dans des systèmes prévoyant le blocage sur une base légale, le législateur interdit souvent explicitement le blocage excessif. Ou encore les utilisateurs n'ont simplement pas intérêt à prendre des mesures compliquées et coûteuses sur le **plan juridique** pour contrer le blocage d'informations particulières qui peuvent être trouvées ultérieurement ou sur une autre page du web. Cet argument est certainement vrai pour tous les systèmes. Le **manque d'efficacité** du blocage est également un argument de taille en faveur de la liberté de l'information. Les autorités nationales de surveillance de la plupart des pays ne visaient pas spécialement le blocage illégal, ni semblent avoir assuré elles-mêmes le blocage (par exemple en Roumanie, en Italie ou au Portugal).

Comme mentionné plus haut, **l'UE a interdit le blocage sans base légale fin 2016** et à la toute fin de la période prévue pour l'élaboration de la présente étude. Un recours sera prévu pour les utilisateurs et un contrôle sur les FSI par les autorités nationales. Il conviendra d'attendre pour voir si les développements ultérieurs confirment cette première évaluation de la toute nouvelle réglementation de l'UE sur l'accès à un internet ouvert. Il conviendrait également d'attendre si les États non membres de l'UE suivent des voies similaires. Les mesures de l'UE semblent proposer une piste prometteuse pour avancer.

40. N° 64 de l'Arrêt.

41. Voir Hessbruegge, *Human Rights Violations Arising from Conduct of Non-State Actors*, Buffalo Human Rights Law Review, Vol. 11 (2005), 21-88, réédité dans Clapham, *Human Rights and Non-State Actors*, 2013, p. 87, 119, 125 : de nombreux "pays ont commencé à externaliser des services assurés jusque-là par des autorités publiques, par exemple la fourniture d'électricité ou d'eau". Les sociétés paraétatiques peuvent être des agents *de jure* de l'Etat. Le facteur décisif en la matière est la fonction publique qu'elles assurent. Cette doctrine est également appliquée (dans une certaine mesure ?) à la liberté d'expression et aux journaux (voir p. 127). L'exécution de toute mesure de blocage devrait être considérée comme une fonction publique. En cas de blocage pour violations du droit d'auteur, cette mission est même prévue par la loi. A côté de ça, la doctrine des agents de facto s'applique : "Si l'État donne au dirigeant une instruction qui est motivée par des raisons politiques, il exerce alors un contrôle effectif. Cela peut s'appliquer aux FSI qui sont aux mains de l'État ou sur lesquels l'État exerce une influence substantielle en tant que propriétaire."

42. Voir les affaires de la Cour européenne des droits de l'homme *Costello-Roberts c. R-U.* (247-C, ser. A, 1993 : châtiments corporels dans une école privée) et *Van der Musselle c. Belgique* (70, ser. A, 1983 : les associations d'avocats doivent assurer l'aide judiciaire conformément à l'article 6 point 3 de la CEDH). Dans les deux cas, les associations privées avaient agi au nom de l'État.

2.2. Retrait de contenus par un hébergeur⁴³

2.2.1. Retrait et blocage : subsidiarité

Normalement, la première mesure serait une ordonnance de retrait à l'encontre d'un hébergeur si ce dernier a son siège ou sa résidence sur le territoire de l'État qui prend la mesure de retrait. Ce retrait mettrait fin à la dissémination d'informations illégales dans l'État ordonnant la mesure et aussi dans d'autres États (où ce type d'information pourrait ne pas être illégal, ce qui poserait un problème en matière de liberté de l'information). Or, aucun État ne peut être obligé à tolérer l'illégalité sur son territoire et la diffusion de ce type d'informations ne peut alors se poursuivre qu'à partir d'un autre État (où l'information est légale).

Ceci mène à la deuxième mesure décrite ci-dessus (2.1) dans ce rapport, à savoir le blocage. Le blocage est en général prononcé à l'encontre d'informations étrangères pénétrant sur le territoire depuis l'étranger ; la différence entre les deux mesures est davantage de nature factuelle : le retrait ne peut être ordonné qu'à l'encontre d'un hébergeur situé sur le territoire de l'État ordonnant la mesure ; le blocage ne peut être ordonné qu'à l'encontre de FSI nationaux et concerne les hébergeurs étrangers et souvent des fournisseurs étrangers de contenus. Toutefois, il peut aussi être difficile de mettre la main sur un hébergeur national. Le fournisseur de contenus peut être anonyme. Néanmoins, pour éviter le problème de l'inefficacité technique du blocage (**proportionnalité**), on pourrait passer par la nécessité d'une hiérarchie entre le retrait et le blocage : le blocage ne peut être ordonné que si le retrait n'est pas possible, ni sur le plan pratique, ni sur le plan technique, ou que de considérables efforts en vue du retrait n'ont rien donné. Certains États soutiennent cette subsidiarité du blocage, comme l'a fait par exemple récemment le BGH allemand dans son récent arrêt de blocage pour violation des droits d'auteur (voir plus haut A.4.1). Un tel raisonnement se comprend dans la perspective des droits de l'homme pour ce qui est de la **proportionnalité**.

Dans la perspective des droits de l'homme, le blocage devrait plutôt être interdit ou restreint à des affaires très graves. Le retrait de contenu manifestement illégal à la source et par l'hébergeur lui-même devrait être plutôt encouragé. Le retrait de contenu en cas de doute sur l'illégalité devrait être soumis à une décision préalable. Les conditions et mécanismes d'un tel retrait devraient être aussi clairs, précis et effectifs que possible⁴⁴.

Étant donné l'inefficacité du blocage, les États tendent à appliquer des mesures nationales de retrait à l'encontre des hébergeurs et s'efforcent de parvenir à une coopération internationale pour le **retrait transfrontalier** (par exemple le réseau INHOPE contre des contenus pédopornographiques, la sollicitation d'enfants en ligne à des fins sexuelles, le discours de haine, la protection des enfants en ligne)⁴⁵. Du point de vue des droits de l'homme, on ne peut que se réjouir de ces évolutions.

2.2.2. Trois approches de base pour le retrait et leurs implications en matière de droits de l'homme

Sous l'angle des droits de l'homme, une importante question se pose concernant le retrait (tout comme le blocage) : quel est le niveau de base légale que l'on peut considérer comme **suffisant** au titre du droit interne

43. Voir en général: Verbiest/Spindler/Riccio/Van der Perre, *Study on the liability of internet intermediaries* (2007) - http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf; il est étonnant de voir que l'étude de Spindler reste autant d'actualité encore aujourd'hui. Les grands problèmes liés à l'hébergement sont restés les mêmes sur quasiment dix ans, à savoir qui peut être considéré comme un hébergeur, quand un hébergeur a-t-il connaissance de contenus illégaux (ou quand peut-il être présumé savoir) et qui est compétent pour donner une notification (par exemple en matière de discours de haine, uniquement des officiers publics ou également des personnes privées). On trouvera d'autres informations de nature comparative dans Spindler/Börner (Hrsg.), *E-Commerce-Recht in Europa und den USA*, 2003 ; Holzngel, *Notice and Take-Down Verfahren als Teil der Providerhaftung*, 2013 (droit américain et allemand, avec des propositions très intéressantes pour une procédure de N&R pour le droit allemand) voir aussi Berger-Walliser, *Die Haftung von Host Providern für Rechtsverletzungen durch Dritte: Vergleich der deutschen und französischen eBay-Rechtsprechung*, ZEuP 2011, 476 ; pour l'affaire *Delfi* et une possible réforme du privilège existant ainsi que des observations de nature comparative voir Fötschl, *Das Haftungsprivileg des Host-Providers auf dem Prüfstand*, MR-Int 2015, p. 47. Pour de nombreuses autres références comparatives, voir Wang, *Development of Hosting ISPs' Secondary Liability for Primary Copyright Infringement in China* – comparaison avec les choix américain et allemand, IIC 2015, 275, et Matulionyte/Nérison, *La solution française d'un havre pour les FSI, comparée aux choix américain et allemand*, IIC 2011, 55.

44. Voir les conclusions du rapport de Freedomhouse sur internet, 2015, p. 13 : "Les gouvernements qui avaient déjà largement étendu leur arsenal d'outils pour contrôler le monde en ligne – en perturbant les réseaux des TIC, en bloquant et en filtrant les contenus et en menant une surveillance invasive – sont actuellement en train de renforcer leur application de ces méthodes. Le blocage étant devenu moins efficace, les gouvernements recourent à la censure du contenu par des requêtes de retrait ou des tactiques coercitives plus puissantes".
Source: https://freedomhouse.org/sites/default/files/FH_FOTN_2015Report.pdf.

45. <http://www.inhope.org/gns/internet-concerns/overview-of-the-problem/illegal-content.aspx>.

pour un retrait ? Ce retrait est une restriction de la liberté d'expression et le test de l'article 10 s'applique (voir ci-dessus, 2.1, Introduction générale).

Le SICL distingue trois systèmes selon leur base légale⁴⁶. Toutefois, différents modèles coexistent. Le modèle du coauteur coexiste souvent avec l'autorégulation (voir Allemagne). Une telle coexistence se retrouve également pour les procédures de N & R (notification et retrait) et l'autorégulation (voir par exemple le Royaume-Uni, qui a adopté une législation spécifique pour le retrait concernant uniquement certains domaines particuliers et applique en parallèle des mesures d'autorégulation ou permet le retrait «sauvage»⁴⁷).

2.2.2.1. Le modèle du coauteur et le privilège d'exonération de responsabilité pour l'hébergeur

La première approche peut être considérée comme le **modèle du coauteur**. L'idée de base est que les règles traditionnelles sur les coauteurs en droit civil, pénal, voire administratif, peuvent servir de base légale pour ordonner le blocage ou le retrait par un hébergeur. Dans ces systèmes, un hébergeur est qualifié de coauteur avec le fournisseur de contenu. Ce modèle est extrêmement large. Il est souvent lié au privilège d'exonération de responsabilité de l'hébergeur. Ce privilège n'est généralement pas restreint à des contenus spécifiques⁴⁸ et s'applique à toutes sortes de contenu illégal.

Or, la **Directive sur le commerce électronique** ne stipule elle-même rien concernant une responsabilité en tant que coauteur. Si (et seulement si) le droit interne d'un État le prévoit, l'hébergeur peut être considéré comme coauteur conformément aux conditions nationales. L'idée de base du **privilège de l'hébergeur** selon la Directive sur le commerce électronique⁴⁹ est que tout État membre de l'UE doit simplement veiller à ce qu'il n'y ait aucune responsabilité civile, pénale ou administrative pour les hébergeurs, si et dans la mesure où l'hébergeur n'a pas réellement connaissance du contenu illégal (quelle que soit sa nature); dès lors que l'hébergeur a connaissance de ce type de contenu, il doit réagir au moment opportun. Si le FSI ou l'hébergeur n'agit pas, alors même qu'il avait connaissance de l'illégalité du contenu, il pourrait dans tous les cas être considéré comme coauteur au sens pénal, administratif ou civil si le droit national (et non le droit européen) le prévoit ou permet ce type de conséquences⁵⁰.

Ce type de règles pénales, administratives et de responsabilité civile semble apparemment très répandu et est bien connu dans vraisemblablement **tous les systèmes juridiques des États membres** de l'UE et du Conseil de l'Europe. En particulier, les systèmes dotés de codifications générales (Codes pénaux, Codes civils, Codes de procédure administrative) sur ces questions tendent à disposer de règles de ce type en matière de coauteur. Toutefois, pour des raisons plus factuelles, la jurisprudence émanant de ces systèmes se concentre sur des questions comparables à l'approche plus restreinte de N & R (à savoir violations des droits d'auteur, diffamation et discours de haine). Il semble que de nombreuses législations nationales d'États membres de l'UE aient «opté» pour ce modèle, peut-être de manière inconsciente. Elles ont simplement formulé leurs règles applicables aux hébergeurs de manière très semblable aux dispositions de la Directive sur le commerce électronique, mais elles n'ont pas adopté de procédure spécifique de N & R. On cite en exemple de cette approche l'Allemagne et l'Autriche.

L'inconvénient de cette approche est l'absence de règle juridique précise. Cela pose dès lors problème puisque la situation n'est pas claire dans la pratique. Ainsi, pour le ministre de la Justice allemand, les discours de haine doivent être retirés par l'hébergeur. Si celui-ci ne le fait pas, il risque de voir sa responsabilité pénale engagée⁵¹. Pour d'autres, les discours de haine sont essentiellement protégés par la liberté d'expression et ne pourraient tout simplement pas être retirés⁵².

46. Cette catégorisation ne diffère que légèrement du rapport Spindler (qui utilise les procédures N&R codifiées, l'autorégulation, la co-régulation, p. 106).

47. Voir le rapport pays R.-U. points 2.2. et suivants.

48. Cependant, actuellement la Suisse n'envisage d'adopter un privilège de l'hébergeur que pour des violations de droits d'auteur. Un privilège de l'hébergeur plus restreint semble aussi en place aux États-Unis (Voir e.g. *Holznapel*, loc. Cit., p. 5 et suivantes).

49. Article 14.

50. La Commission européenne a annoncé à la mi-2015 une réforme de la loi pour les fournisseurs de services sur internet, y compris les fournisseurs d'hébergement (voir ci-dessus, 2.1.3.2. sur "*Stratégie pour un marché unique numérique*"). Certains signes indiquent que la situation va évoluer de privilèges (formulés négativement) en matière de responsabilité vers une procédure plus positive de N & R formulée et précise avec des conditions et sauvegardes procédurales différentes selon le contenu qui devrait être retiré (ainsi, les contenus ayant causé les violations les plus graves doivent être retirés immédiatement par l'hébergeur; dans des situations peu claires, un tribunal doit d'abord rendre une décision pour sauvegarder la liberté d'expression; des règles précises sur la position à adopter en cas de discours de haine). Si (et seulement si) une nouvelle procédure N & R – UE est strictement suivie, l'hébergeur sera récompensé par une exonération de responsabilité.

51. Maas, *Löschpflicht für Hasskommentare?*, ZRP 2015, 222.

52. Härting, *Löschpflicht für Hasskommentare?*, ZRP 2015, 222: „Erst die Kenntnis von solchen Rechtsverstößen verpflichtet zum Handeln. Dies aber auch nur, wenn es tatsächlich um eine Rechtsverletzung geht (zB Volksverhetzung), nicht jedoch bei jedem beliebigen „Hasskommentar“).

2.2.2.2. Autorégulation

Pour traiter la possible violation d'autres droits fondamentaux, de nombreux États ont opté pour l'*autorégulation*. Un très bon exemple récent nous est donné par l'Allemagne et la lutte contre le discours de haine en lien avec la crise des réfugiés (Groupe de travail contre le discours de haine)⁵³. Des codes de conduite similaires (codecs) ont été adoptés dans de nombreux États⁵⁴. Dans certains d'entre eux, ils semblent même avoir des effets en justice (voir par exemple la Belgique et les Pays-Bas⁵⁵). Toutefois, dans d'autres, ils ne sont que des instruments de droit souples entre des parties intéressées à l'autorégulation, mais n'ont aucune force contraignante dans des litiges entre un détenteur de droits ou une personne victime de diffamation et un hébergeur (ou du moins n'apporte pas de solution dans des affaires critiques, par exemple en Autriche⁵⁶).

2.2.2.3. Procédures de N & R prévues en droit

Le modèle suivant trouve sa source dans l'idée que les dispositions relatives aux coauteurs (ou la jurisprudence en la matière) ne forment pas une base légale suffisamment claire pour que des mesures de retrait puissent être menées par un hébergeur. Pour que ces mesures puissent être prises, il faudrait des **lois et règlements très spécifiques (et nouveaux)** visant directement les hébergeurs et leur expliquant très clairement ce qu'ils peuvent retirer et ce qu'ils doivent retirer (et ce qu'ils ne peuvent pas retirer).

Les meilleurs **exemples** que l'on peut trouver ici sont ceux de la Finlande⁵⁷, de la Hongrie⁵⁸, de la Lituanie⁵⁹, de la France⁶⁰, de la Suède⁶¹ et partiellement du Royaume-Uni où il existe des obligations spécifiques de retrait mais uniquement pour certains secteurs particuliers (par exemple contenu encourageant le terrorisme, la pédopornographie et contenu obscène entre adultes, atteinte à l'ordre public et à des communications ciblées, diffamation, informations confidentielles)⁶².

53. Le ministre allemand de la Justice a formé une task force spéciale contre le discours de haine qui a présenté ses mesures mi-décembre 2015 ("*Ensemble contre le discours de haine: moyens proposés par la Task force contre le discours de haine pour s'attaquer au discours de haine illégal en ligne*"). Voir http://www.bmjv.de/SharedDocs/Artikel/DE/2015/12152015_ErgebnisrundeTaskForce; les principales conclusions sont les suivantes:

« Les participants à la task force sont tous mus par la conviction qu'il n'y a pas de place pour le discours de haine sur les médias sociaux. Les discours de haine doivent être contrés en faisant front, tous ensemble, le secteur des affaires, la société civile et les décideurs politiques.

Les participants de la task force affirment que tous types de discours de haine prohibés par le droit allemand seront analysés et retirés sans délai après notification ("*nach Inkenntnissetzung*"). Les sociétés représentées au sein de la task force ont arrêté une série de bonnes pratiques et d'objectifs ... , qui devraient guider les entreprises du net pour qu'elles assurent un traitement rapide et effectif des signalements de contenus illégaux, ou de contenus qui contreviennent aux termes et conditions d'une société, tout en assurant aussi une étroite collaboration à cet égard avec les organisations de la société civile.

La liberté d'expression est vitale pour le processus démocratique. Elle protège toutes les expressions légitimes d'opinion, quand bien même elles sont discutables. Tous les acteurs sociaux sont invités à refuser fermement la propagande raciste et les préjugés xénophobes. Pour cela, le contre-discours est un instrument efficace et il faut un engagement citoyen. Les sociétés et organisations de la société civile représentées au sein de la task force sont prêtes à unir leurs forces dans ce but.

Toutes les mesures visant à lutter contre le discours de haine devraient être envisagées à la lumière des droits de l'homme. Les parties prenantes soulignent que la liberté d'opinion et la liberté d'expression sont des conditions indispensables pour le plein épanouissement personnel. Elles sont essentielles pour toute société et constituent le socle de toute société libre et démocratique» http://www.bmjv.de/SharedDocs/Downloads/DE/Artikel/12152015_TaskForceErgebnispapier_eng.pdf?__blob=publicationFile&v=2.

54. Voir les rapports pays point 2.2.

55. Voir le rapport pays Pays-Bas, point 2.2: même si la procédure N & R peut être considérée comme une forme d'autorégulation, la non-conformité avec la procédure juridique entraînera l'engagement de la responsabilité civile ou pénale, plaçant l'hébergeur dans le cadre réglementaire formel.

56. Voir [https://www.ispa.at/wissenspool/positionspapiere/ispa-position.html:„Für andere Kategorien vermeintlich rechtswidriger Inhalte \(wie z.B. die unerlaubte Verbreitung urheberrechtlich geschützten Materials, Online-Glücksspiel, Diffamierung, Terrorismus etc.\) stellt die Selbstregulierung nicht die ideale Lösung dar. Ein Provider ist nämlich nicht dazu in der Lage sich ein Urteil über die Rechtmäßigkeit oder Unrechtmäßigkeit derartiger Inhalte zu bilden.“](https://www.ispa.at/wissenspool/positionspapiere/ispa-position.html:„Für andere Kategorien vermeintlich rechtswidriger Inhalte (wie z.B. die unerlaubte Verbreitung urheberrechtlich geschützten Materials, Online-Glücksspiel, Diffamierung, Terrorismus etc.) stellt die Selbstregulierung nicht die ideale Lösung dar. Ein Provider ist nämlich nicht dazu in der Lage sich ein Urteil über die Rechtmäßigkeit oder Unrechtmäßigkeit derartiger Inhalte zu bilden.“) Ces déclarations ont été faites pour le blocage, mais s'appliquent aussi aux activités d'hébergeur.

57. Il doit y avoir une ordonnance judiciaire ou une procédure spécifique pour violation de droits d'auteur doit avoir été suivie. Toutefois, l'hébergeur doit retirer de son propre chef les contenus suivants (une fois qu'il en a eu connaissance): discours de haine (tel que réglementé dans le Code pénal) diffusion d'images pédopornographiques, de violences sexuelles ou de relations sexuelles de nature zoophile. (Voir Section 184 du Code de 2015 sur la société de l'information, rapport pays Finlande, 2.2).

58. Voir rapport pays Hongrie, point 2.2.3.

59. Voir rapport pays Lituanie, point 2.2.

60. Voir rapport pays France, point 2.2.

61. Voir loi suédoise sur les sites d'affichage, rapport pays Suède, 2.2.

62. Voir rapport pays R.-U. points 2.2.1 à 2.2.5. Toutefois, un tel régime spécifique ne devrait pas permettre l'existence parallèle de retrait "sauvage", comme c'est le cas au Royaume-Uni. Voir rapport pays R.-U. point 2.2: bien qu'il n'y ait pas d'autre disposition statutaire en droit pénal ou civil qui prévoient le retrait de contenu illégal en ligne, il est signalé que bon nombre d'hébergeurs retirent ce type de contenu indépendamment de la légitimité de la plainte afin de mieux se protéger contre l'engagement de leur responsabilité.

Du point de vue des **droits de l'homme**, ce modèle constitue à l'évidence une avancée. Ce système de N & R pourrait, en matière d'illégalité de contenus, s'appuyer sur le modèle du coauteur ou énumérer de manière autonome des raisons spécifiques pour un retrait, cette dernière possibilité étant plus convaincante. De fait, ces modèles restreignent considérablement le volume et la quantité de contenus qui doivent être retirés. Toutes les illégalités, comme dans le modèle du coauteur, ne peuvent pas servir de base pour un retrait. Le retrait doit être justifié de manière appropriée. Ce type de modèle respecte dès le départ les normes des droits de l'homme. De plus, ces régimes spécifiques clarifient les mesures qu'un hébergeur peut prendre de son propre chef et celles qu'il ne peut prendre que sur production d'une ordonnance d'un tribunal ou d'une ordonnance d'une autorité administrative (l'autorité de surveillance).

2.2.2.4. Droit des médias appliqué aux hébergeurs

On a déjà mentionné que le modèle du coauteur a été critiqué car n'étant pas suffisamment spécifique en tant que base légale au sens de l'article 10 de la Convention européenne des droits de l'homme. Il semble avoir également rencontré de sérieuses objections au niveau du droit matériel national. Le premier problème est que l'application des règles relatives aux coauteurs pour les hébergeurs semble très étendue. Toutes sortes d'illégalités pourraient ainsi être reprochées à un hébergeur. Et ce modèle est particulièrement sévère si de graves violations pénales sont en jeu (par exemple pédopornographie, propagande nazie ou terroriste). Les tribunaux de certaines juridictions étaient plutôt réticents à considérer les hébergeurs comme des auteurs pour ce type de gravité.

Certains États (à savoir la Russie, la Pologne, la Hongrie et l'Autriche) ont commencé à appliquer (toutes sortes de) dispositions de **leurs législations concernant les médias ou la presse** aux hébergeurs sur leur territoire ou créé de nouvelles lois sur les médias électroniques dont le contenu est similaire à celui des lois sur les médias traditionnels (par exemple en Russie). Ainsi, les hébergeurs sont souvent caractérisés comme étant des éditeurs au sens de la loi sur la presse. Les hébergeurs sont également menacés de voir leur responsabilité engagée dans des cas tels que ceux applicables à une société de presse ou un éditeur (**obligations de diligence** pour les contenus et dispositions spécifiques relatives à celui-ci, par exemple sur la diffamation ou les discours de haine⁶³)⁶⁴. Ce développement est intervenu essentiellement du fait que les hébergeurs étaient trop passifs dans le retrait de contenu ou attendaient d'être notifiés par des tierces parties.

2.2.3. Une évaluation axée sur les droits de l'homme des approches concernant les activités d'hébergeur

Le principe de base devrait être qu'il n'y a pas de différence de principe entre les **affaires en ligne et hors ligne**⁶⁵. Le simple fait que l'on puisse toucher un plus large auditoire en ligne et donc causer davantage de dommages ne devrait pas directement et uniquement aboutir à des évaluations différentes en matière de droits de l'homme.

2.2.3.1. Autorégulation

Sous l'angle des droits de l'homme, cette autorégulation est confrontée à la même critique que le blocage sur la base volontaire, à savoir qu'elle ne constitue pas une base légale solide (« prévue par la loi ») aux termes de l'article 10 § 2 de la Convention européenne des droits de l'homme.

63. Pour une étude comparative très complète sur le discours de haine, la loi sur les médias et la liberté d'expression, voir *The European legal framework on hate speech, blasphemy and its interaction with freedom of expression*, September 2015, PE 536.460 (version anglaise).

64. Il convient de mentionner que, ce faisant, les États membres de l'UE ont aussi commencé en partie à **saper le privilège du fournisseur de services d'hébergement** et créé des obligations et des responsabilités pour les hébergeurs qui pourraient aller plus loin que ce qu'autorisait la Directive sur le commerce électronique, à savoir assurer une surveillance du contenu, s'abstenir de publier des contenus problématiques, procéder à un retrait avant ou sans notification. En un tel cas, il y a conflit entre des dispositions du droit, ce qui pose problème au regard de l'élément "prévu par la loi" (comme par exemple dans l'affaire *Delfi* que la Cour de Strasbourg a eu à connaître). Toutefois, tant que des obligations d'une société de médias en ligne sont interprétées en conformité avec le privilège du prestataire de services d'hébergement (comme c'est le cas pour l'instant en Autriche – voir contribution nationale, point 2.2. sur l'application de la Loi sur les médias aux médias en ligne), il ne devrait pas y avoir d'obstacle pour l'application de cette approche qui n'apporte rien de mieux et ne nuit pas non plus.

65. Voir *Fatullayev c. Azerbaïdjan*, 22 avril 2010, requête n° 40874/07. Pour cette affaire, voir les informations très instructives dans le rapport pays pour l'Azerbaïdjan. Voir aussi Benedek/Kettmann, *Freedom of Expression and the Internet*, p. 88, 91, ainsi que pour le « libel tourism ». Pour le cas particulier des réseaux sociaux, voir Benedek/Kettmann, loc. Cit., p. 98.

Plus important, l'autorégulation encourage la suppression excessive. Nous en avons des exemples (en Pologne⁶⁶ ou encore en Norvège⁶⁷) lorsque des hébergeurs ont commencé à supprimer du contenu de **leur propre chef** (« **suppression excessive** » **sauvage**) pour éviter tout risque. Ce risque est inhérent à ce modèle qui pose donc des **problèmes en matière de droits de l'homme**.

2.2.3.2. Le modèle du coauteur

Comme déjà mentionné plus haut, le **modèle du coauteur** est fortement lié **au privilège des fournisseurs de services d'hébergeur** tel qu'adopté et mis en pratique par de nombreux États membres de l'UE. Ce privilège contient également une sorte **d'évaluation inhérente des droits de l'homme**. Il repose sur l'idée que les règles applicables aux coauteurs (indirectement) aboutissent à la suppression, puisqu'elles pourraient entraîner la sanction du FSI ou de l'hébergeur ou l'engagement de leurs responsabilités (que ce soit sur la base de la connaissance effective ou de la passivité). Sinon, un hébergeur continuerait simplement de commettre la violation de la loi qui pourrait entraîner des mesures supplémentaires, parfois même jusqu'à l'annulation de la licence d'un hébergeur dans un pays donné. Dans la mesure où un hébergeur est **obligé** de retirer du contenu (pour que sa responsabilité ne soit pas engagée), il doit également être **autorisé** à effectuer ce retrait. Pour mettre un terme à la co-commission, l'hébergeur devrait retirer le contenu **de son propre chef**. En principe, selon la Directive, il n'est besoin d'aucune décision de justice pour cela. Toutefois, elle ne le précise pas de manière explicite. La deuxième question inhérente aux droits de l'homme liée au privilège de l'hébergeur est que la liberté d'expression se voit accorder une portée extrêmement large pour aussi longtemps que l'hébergeur n'a pas reçu de notification. C'est là encore un raisonnement basé sur les droits de l'homme consacré dans le privilège de l'hébergeur prévu par la Directive sur le commerce électronique.

Dans la perspective de **l'article 10 de la Convention européenne des droits de l'homme, le modèle du coauteur** pourrait poser quelques problèmes pour ce qui est de la base légale pour une suppression. Ces règles ne sont pas suffisamment **spécifiques** pour traiter directement du cas des hébergeurs. La prémisse de base que l'hébergeur peut supprimer de son propre chef du contenu pourrait être problématique également du point de vue de la liberté d'expression.

Le **test de l'article 10** à cet égard fait référence aux règles nationales applicables au coauteur en droit pénal, administratif et civil et aux délits correspondants commis par le fournisseur de contenu. Dans chacune des affaires, le test des buts légitimes doit être appliqué. Il pourrait y avoir de nombreuses situations où ce type de règles ne satisferait pas ce test. Une règle matérielle spécifique pourrait s'inscrire dans le droit fil de la Convention européenne des droits de l'homme. Mais en combiné avec la situation relative aux coauteurs et l'article 10 de la CEDH, le test est différent et vraisemblablement plus resserré.

Pour ce qui est de la **nécessité** dans une société démocratique, des buts légitimes et de la proportionnalité, il semble que cela pose beaucoup moins de problèmes en cas de retrait qu'en cas de blocage. Les principales affaires relatives à l'hébergement concernent des violations des droits d'auteur dans des applications web 2.0, la diffamation, la calomnie et les discours de haine. Les violations des droits d'auteur constituent des violations du « droit d'un tiers ». Tant qu'il y a une **personne privée** lésée à titre individuel, l'objectif légitime sera la « réputation d'autrui ». Dans les affaires de discours de haine et affaires connexes, on pourrait envisager le « maintien de l'ordre » ou la « protection de la morale ». Mais dans ces cas, les frontières deviennent très minces et la notification pourrait devoir provenir d'une autorité.

Ceci est particulièrement vrai en **droit pénal**. Le caractère pénal de la pornographie infantile ou du contenu terroriste est clair. Il est clair également que le fournisseur de contenu commet une telle infraction. Toutefois, il semble beaucoup moins convaincant que l'hébergeur (ou une société de médias signalant ce type d'activité) a commis un tel délit en tant que coauteur (même s'ils avaient connaissance du contenu et n'ont pas agi). Une bonne partie de l'analyse va dépendre de l'approche nationale en ce qui concerne les coauteurs et des conditions requises pour prouver leur intention de commettre un tel délit. Certains systèmes peuvent avancer que l'omission par l'hébergeur doit se produire avec l'intention de soutenir activement le fournisseur de

66. Voir notamment le rapport pays sur la Pologne, point 2.2.1, pour les conséquences de l'absence de procédure de N & R spécifique : cette situation a un effet **dissuasif** non souhaité qui fait que les fournisseurs de services intermédiaires du net retirent tout contenu pouvant créer la controverse et signalé comme potentiellement illégal pour éviter toute responsabilité.

67. Voir le rapport sur la Norvège point 2.2.3 : certains hébergeurs ont conçu des **contrats utilisateurs** qui permettent à l'hébergeur de retirer tout contenu controversé, y compris du **contenu qui n'est pas illégal**, pour ne pas voir leur responsabilité engagée dans tout litige concernant le contenu. Par exemple, un auteur évoque un incident en février 2008 où l'hébergeur norvégien Imbera a retiré des images des « **caricatures de Mahomet** » danoises des sites web de l'un de ses clients, une organisation appelée Human Rights Service. Le motif invoqué pour ce retrait était que le contrat d'utilisateur d'Imbera interdisait de télécharger des contenus controversés sur les serveurs d'Imbera.

contenu. Le fait que l'hébergeur se soit par pure **paresse** ou par surcharge de travail abstenu d'agir pourrait ne pas suffire pour en faire un coauteur.

Toutefois, dans bon nombre d'États membres de l'UE, dans le cadre de la mise en œuvre de la Directive de l'UE sur le commerce électronique, il a été créé une obligation générale pour l'hébergeur d'agir une fois qu'il a eu connaissance du caractère illégal d'un contenu. Ce faisant, l'hébergeur peut être considéré comme coauteur de toute infraction. De sérieux doutes demeurent sur le fait de savoir si une telle approche devrait être suivie⁶⁸. Menacer un hébergeur de voir sa responsabilité engagée en droit pénal ou civil à titre de coauteur pourrait aboutir à un excès de retraits. Toutefois, il semble qu'il n'y pas eu beaucoup d'affaires dans lesquelles un hébergeur aurait réellement dû faire face à de telles conséquences.

Le principe très large du coauteur s'est heurté à une certaine restriction. La principale question consiste à savoir si le contenu ou commentaire spécifique est illégal, ce qui peut être délicat à évaluer. C'est pourquoi certains systèmes nationaux ou jurisprudences nationales ont restreint l'obligation pour l'hébergeur de retirer des contenus de son propre chef dans des cas concernant des contenus « manifestement » illégaux (voir par exemple les règles de la Belgique relatives à l'hébergement⁶⁹ ou les nouvelles règles finlandaises sur ce sujet, et, en Autriche, une telle restriction émane de la jurisprudence). Pour d'autres contenus « normalement » illégaux, il faudrait des mesures supplémentaires ou une ordonnance du tribunal avant de pouvoir les retirer.

2.2.3.3. Législation relative à la notification et retrait

Il est sûrement plus approprié de se doter d'une **législation spécifique de N & R** et de règles spécifiques sur le retrait de contenus précis. Dans la perspective des droits de l'homme, il pourrait même être nécessaire de mettre en place un régime spécifique de cette nature.

68. Voir sur ce point le rapport pays sur l'Azerbaïdjan concernant les activités d'hébergement et le matériel pertinent de la Cour européenne des droits de l'homme.

69. Voir n° 2.1. du rapport pays pour la Belgique.

Dans les différents États membres du Conseil de l'Europe, le blocage et la suppression de contenus en ligne sont souvent traités de façon similaire. Cependant, l'existence ou non d'un cadre législatif spécifique à l'internet et les caractéristiques des « modèles » réglementaires se traduisent par des pratiques différentes et peuvent placer les États concernés devant certaines difficultés.

Le Conseil de l'Europe a commandé à l'Institut suisse de droit comparé une étude comparative sur le filtrage, le blocage et la suppression de contenus illégaux sur l'internet dans ses 47 États membres. Cette étude décrit et évalue les cadres législatifs ainsi que la jurisprudence et la pratique dans le domaine. Elle comprend une analyse comparative des rapports nationaux qui permet de révéler des tendances en Europe ainsi que d'éventuelles lacunes – objet de cette publication, et des rapports par pays (disponibles sur le site web HYPERLINK "<http://www.coe.int/freedomof>" www.coe.int/freedomof expression).

www.coe.int

Le Conseil de l'Europe est la principale organisation de défense des droits de l'homme du continent. Il comprend 47 États membres, dont les 28 membres de l'Union européenne. Tous les États membres du Conseil de l'Europe ont signé la Convention européenne des droits de l'homme, un traité visant à protéger les droits de l'homme, la démocratie et l'État de droit. La Cour européenne des droits de l'homme contrôle la mise en œuvre de la Convention dans les États membres.