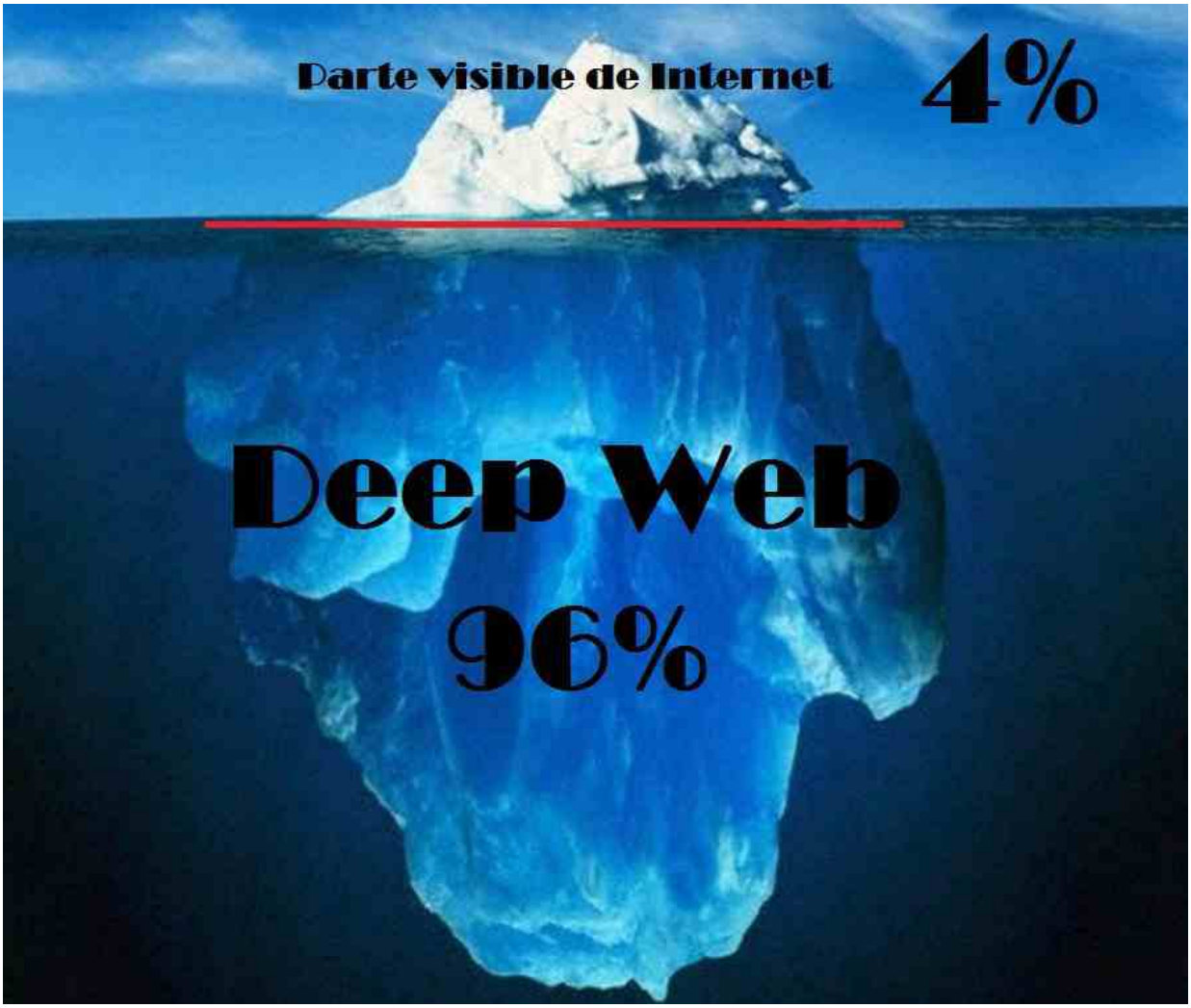
Mont St-Martin 45

4000 LIEGE

LA CYBERCRIMINALITÉ,
LES INFRACTIONS RELATIVES
AUX CONTENUS ILLICITES ET PRÉJUDICIABLES



Michael Lopez

Troisième baccalauréat en droit

Année académique 2014-2015

REMERCIEMENTS

J'adresse mes remerciements à mon promoteur, Maître Petré, pour sa disponibilité et son aide.

Je voudrais aussi remercier toutes les personnes qui ont contribué de près ou de loin à l'élaboration de ce travail.

PLAN

INTRODUCTION

De nos jours, nous utilisons presque tous internet. Cet outil de communication est devenu indispensable pour bon nombre d'entre nous, en particulier chez les jeunes qui passent en moyenne deux heures par jour sur le net. Mais le net a aussi créé une porte d'accès à un nouveau genre de criminalité: la cybercriminalité, qui provoque déjà énormément de dommages.

D'une part, selon une enquête de "Norton by Symantec", la cybercriminalité coûterait environ 3,5 milliards d'euros par an aux entreprises belges. Par exemple, les cybercriminels dérobent des données sensibles afin de faire chanter les grosses entreprises. D'autre part, en 2010, près de 1,4 millions de Belges ont été touchés par la cybercriminalité, soit trois Belges par minute.

Mais pourquoi la cybercriminalité prend-elle autant d'ampleur? Il existe à la fois des causes juridiques et non juridiques. Tout d'abord, la portée internationale du phénomène par le biais du web: le problème de cette portée internationale trouve son origine dans le fait que chaque État ne sanctionne pas les mêmes contenus illicites. Ensuite, notons la difficulté de rassembler des preuves contre le ou les auteurs. Et enfin, citons la rapidité et l'anonymat que confère internet pour commettre l'infraction. En effet, il est facile de commettre une infraction sur le net en quelques clics et sous un pseudonyme qui n'a aucun sens tel que "Y4fr4d1a". En Belgique, le risque de subir une attaque par internet est de 31 %[1].

Par ailleurs, le droit à la liberté d'expression est garanti par les États. En conséquence, chacun possède le droit de répandre les informations en sa possession et ses idées sur le réseau. Cependant, si les opinions ou les informations publiées nuisent à autrui, l'État doit sanctionner les comportements abusant du droit à la liberté d'expression.

L'objectif de ce TFE est d'apporter un éclairage sur la cybercriminalité, en particulier sur les **contenus illicites**, et sur les moyens dont les victimes disposent pour

[1] Voir annexe n° 1

se défendre contre les contenus qui leur causent un préjudice sur la toile. Ce TFE tentera de répondre aux questions suivantes:

- Jusqu'où va la liberté d'expression?
- Quelles sont les limites à ne pas dépasser au-delà desquelles les États doivent sanctionner afin de maintenir le cyberespace à l'abri des cybercriminels?
- Quels sont les contenus qui peuvent être considérés comme manifestement illicites?
- Qui peut être tenu responsable des contenus illicites et préjudiciables?

Nous tenterons en premier lieu de définir le terme de cybercriminalité, ce qui se cache derrière une appellation si vaste et quel classement nous pouvons faire de toutes les infractions englobées dans ce mot. Ensuite, nous nous interrogerons sur la liberté d'expression. Dans un deuxième temps, nous analyserons les contenus illicites courants et la répression tant sur le plan international que sur le plan national en matière pénale ainsi qu'en matière civile. Pour terminer, nous verrons en détail la responsabilité civile et pénale des intermédiaires du web ainsi que les exonérations de responsabilités possibles.

CHAPITRE 1: DÉFINITION DE LA CYBERCRIMINALITÉ

Il existe beaucoup de définitions de la cybercriminalité. Par exemple, le dictionnaire Larousse définit la cybercriminalité comme:

> *"L'ensemble des infractions pénales commises sur les réseaux de télécommunication, en particulier Internet"*[2].

Mais Symantec, une entreprise connue pour la création de l'antivirus du même nom, s'est basé sur un ensemble de définitions de la cybercriminalité pour arriver au résultat suivant:

> *"Tout acte criminel perpétré à l'aide d'un ordinateur ou sur un réseau, ou à l'aide de matériel informatique"*[3].

Une autre définition plus simpliste consiste à dire que la cybercriminalité est un type de criminalité commis avec un ordinateur. Il n'existe pas encore de définition légale de la cybercriminalité et il paraît compliqué de définir cette notion; c'est pourquoi nous vous proposons cette définition:

La cybercriminalité regroupe un ensemble d'infractions pénales pour la commission desquelles les moyens utilisés sont les réseaux de télécommunication nationaux ou internationaux, particulièrement les ordinateurs et également les GSM disposant d'un accès au réseau ou à l'aide d'un autre matériel informatique.

Dans toutes les définitions, la cybercriminalité est caractérisée par la diversité des infractions que nous détaillerons plus loin dans ce travail, ensuite par la multitude de supports utilisables par les auteurs d'infractions. À titre d'exemple, le routeur ou encore le GSM bénéficiant d'un accès internet est exposé au même risque que les ordinateurs. Le routeur est un intermédiaire entre deux ou plusieurs réseaux informatiques comme les ordinateurs qui leur permet de partager les don-

[2] http://www.larousse.fr/dictionnaires/francais/cybercriminalit%C3%A9/10910062
[3] http://securityresponse.symantec.com/fr/be/norton/cybercrime/definition.jsp

nées. Une attaque réussie sur un routeur présente un grand danger, car le pirate aura accès à toutes les données qui passent entre deux ou plusieurs ordinateurs.

Le terme "cybercriminalité" et les actes des cybercriminels peuvent être rassemblés dans deux types d'atteintes:

Premièrement, citons les atteintes aux biens qui concernent les fraudes et les escroqueries. Par exemple, la vente d'objet volé ou encore un virus qui a pour fonction d'effacer le registre de l'ordinateur, si bien que celui-ci ne peut plus être utilisé. Sans un registre, un ordinateur ne sait plus, notamment, offrir les services du clavier ou de la souris.

Deuxièmement, relevons les atteintes aux personnes qui touchent moralement les citoyens par des contenus illicites, et plus particulièrement, par la publication de contenus préjudiciables et illicites sur la toile. Nous verrons plus loin quels sont ces contenus et comment ils sont sanctionnés en droit belge. Avant, il convient de classer les infractions qui se regroupent sous l'appellation "Cybercriminalité" afin de cibler le sujet de ce travail.

CHAPITRE 2: CLASSIFICATION DES INFRACTIONS EN RAPPORT AVEC LA CYBERCRIMINALITÉ

Plusieurs classements des infractions en rapport avec la cybercriminalité existent. Le classement le plus pertinent a été réalisé par le conseil de l'Europe dans la Convention sur la cybercriminalité signée à Budapest le 23 novembre 2001. Les objectifs poursuivis par le conseil de l'Europe étaient d'harmoniser les législations nationales concernant l'utilisation d'internet dans les différents États, de fournir les moyens nécessaires à la poursuite de la cybercriminalité et de créer une coopération internationale entre les différents États. Cette Convention classe la cybercriminalité en quatre types d'infractions:

1 LES INFRACTIONS CONTRE LA CONFIDENTIALITÉ, L'INTÉGRITÉ ET LA DISPONIBILITÉ DES DONNÉES ET SYSTÈMES INFORMATIQUES

Nous ne comptons pas développer l'ensemble des infractions contre la confidentialité, l'intégrité et la disponibilité des données; nous allons juste vous en donner un léger aperçu. Ce type de cyber-délit rassemble les atteintes au principe de confidentialité, de disponibilité et d'intégrité des données informatiques. Une illustration classique d'acte illicite contraire au principe de confidentialité est l'accès illégal au matériel informatique par piratage.

1.1 L'ACCÈS ILLÉGAL À UN MATÉRIEL INFORMATIQUE

En Belgique, la loi du 28 novembre 2000 relative à la criminalité informatique punit l'accès illégal à un support informatique en ajoutant l'article 550bis dans le Code pénal.

> **Article 550bis**: *"§ 1er. Celui qui, sachant qu'il n'y est pas autorisé, accède à un système informatique ou s'y maintient, est puni d'un emprisonnement*

de trois mois à un an et d'une amende de vingt-six francs à vingt-cinq mille francs ou d'une de ces peines seulement".

Cet article est très important pour pouvoir lutter contre la cybercriminalité puisqu'il interdit l'accès et le maintien de l'accès illégal à un système informatique. Le pirate obtient l'accès à des données privées en craquant le mot de passe d'un ordinateur ou d'un site internet dont il n'est pas le propriétaire.

1.2 L'ALTÉRATION DES DONNÉES INFORMATIQUES

Après l'atteinte à la confidentialité des données par un accès illégal, nous nous attarderons sur les atteintes à l'intégrité et la disponibilité des données. Ces attaques causent un grand préjudice aux entreprises. En effet, une entreprise perd une fortune si un pirate l'empêche d'accéder à sa base de données. Il existe quatre manières de commettre une telle atteinte:

- soit par l'effacement des données,
- soit par la suppression des données,
- soit par la modification des données,
- soit par la limitation de l'accès aux données.

Dans notre pays, c'est toujours la loi du 28 novembre 2000 relative à la criminalité informatique qui punit les auteurs de ces infractions en ajoutant l'article 550ter dans le Code pénal:

> **Article 550ter**: *"§ 1er. Celui qui, dans le but de nuire, directement ou indirectement, introduit dans un système informatique, modifie ou efface des données, ou qui modifie par tout moyen technologique l'utilisation possible de données dans un système informatique, est puni d'un emprisonnement de six mois à trois ans et d'une amende de vingt-six francs à vingt-cinq mille francs ou d'une de ces peines seulement".*

Tout d'abord, le pirate doit modifier ou effacer des données contenues sur un support informatique (élément matériel)[4]. Ensuite, il faut que le pirate agisse avec l'intention de nuire à la victime (dol spécial) pour être sanctionné par l'article 550ter §1er.

Le virus informatique est le cas le plus fréquent d'atteinte à l'intégrité des données. Il s'agit d'une ligne de code malveillante écrite dans un programme et cachée de manière à ce que la victime exécute le programme. Par exemple, un pirate va envoyer un mail aux victimes potentielles en se faisant passer pour un employé de Microsoft. Il va demander aux victimes d'installer une mise à jour de sécurité alors qu'il s'agit d'un virus contenant par exemple une commande "Del c" qui efface l'ensemble du disque dur d'un ordinateur.

Le paragraphe 3 de l'article 550ter vise des attaques informatiques dont le but est de rendre le système informatique indisponible et par conséquent de limiter l'accès aux données:

> **Article 550ter**: *"§ 3. Celui qui, suite à la commission d'une infraction visée au § 1er, empêche, totalement ou partiellement, le fonctionnement correct du système informatique concerné ou de tout autre système informatique, est puni d'un emprisonnement de un an à cinq ans et d'une amende de vingt-six francs à cent mille francs ou d'une de ces peines seulement".*

Ici, le simple fait d'empêcher le fonctionnement d'un système informatique est punissable si les éléments constitutifs[5] visés à l'article 550ter §1 sont réunis. L'exemple type est l'attaque par déni de service qui consiste à empêcher l'accès au système par les utilisateurs autorisés en utilisant autant d'ordinateurs que possible pour accéder au système afin qu'aucune connexion ne soit possible pour les utilisateurs légitimes[6]. Une telle attaque porte un préjudice immense aux entreprises car elles ne disposent plus de l'accès à leurs données.

---

[4] L'élément matériel est la réalisation du fait ou de l'abstention qui est interdit par la loi.
[5] Les éléments constitutifs de l'infraction sont les conditions qui doivent être réunies pour qu'une infraction existe.
[6] Voir annexe n° 2

2 LES INFRACTIONS INFORMATIQUES

Cette famille d'infractions rassemble les délits qui doivent être commis à l'aide d'un système informatique. Le terme "système informatique" désigne aussi bien les ordinateurs que tous les appareils qui possèdent un accès à internet, comme les GSM, I Phone et autres nouveautés technologiques.

Les infractions de fraude informatique, d'hameçonnage et le vol d'identité font partie des infractions informatiques. L'article 5 de la loi du 28 novembre 2000 relative à la criminalité informatique rajoute l'article 504quater dans le Code pénal afin de sanctionner les infractions informatiques:

> **Article 504quater**: *"§ 1er. Celui qui se procure, pour soi-même ou pour autrui, un avantage patrimonial frauduleux en introduisant dans un système informatique, en modifiant ou effaçant des données qui sont stockées, traitées ou transmises par un système informatique, ou en modifiant par tout moyen technologique l'utilisation possible des données dans un système informatique, est puni d'un emprisonnement de six mois à cinq ans et d'une amende de vingt-six francs à cent mille francs ou d'une de ces peines seulement".*

Les éléments matériels de l'article 504quater sont les suivants: d'abord, l'obtention d'un avantage patrimonial, et ensuite, l'utilisation d'un système informatique pour modifier ou effacer des données. Quant à l'élément moral[7], il s'agit d'un dol général.

Cet article est de plus en plus utile depuis l'apparition des banques en ligne où les clients usent de leurs ordinateurs pour effectuer leurs transactions financières. Un pirate pourrait par exemple intercepter les virements et changer le compte bénéficiaire puis renvoyer le virement sur le serveur de la banque afin de recevoir le paiement à la place du bénéficiaire légitime.

[7] L'élément moral est la recherche de la volonté de la personne lorsqu'elle a commis l'acte répréhensible.

3 LES INFRACTIONS LIÉES AUX ATTEINTES À LA PROPRIÉTÉ INTELLECTUELLE

Le droit à la propriété intellectuelle correspond aux droits qu'ont les auteurs sur les œuvres qu'ils ont créées. Ces infractions sont apparues en même temps que la numérisation d'information. Pour comprendre les infractions liées aux atteintes à la propriété intellectuelle, il faut savoir ce que signifie le mot "numériser". Le dictionnaire Larousse en donne une définition très complexe:

> *"Se dit de la représentation d'informations ou de grandeurs physiques au moyen de caractères, tels que des chiffres, ou au moyen de signaux à valeurs discrètes"*[8].

En fait, la numérisation est un procédé qui permet de transformer une information en une suite de nombres pour que l'ordinateur puisse comprendre l'information et la reproduire fidèlement à l'écran. Grâce à ce procédé, la copie de supports sur un ordinateur tels que les DVD ou les CD devient extrêmement facile et précise. Or, les sociétés ont commencé à répandre leurs logos et leurs produits sur internet afin d'améliorer leurs services et se faire connaître sur le net. Cependant, la numérisation donne la possibilité aux pirates de reproduire et de redistribuer les produits d'une entreprise pour une somme modique ou gratuitement. Il existe deux grands types d'atteintes à la propriété sur le net.

L'échange des logiciels et des fichiers protégés entre ordinateurs est la première catégorie d'infraction liée à l'atteinte à la propriété intellectuelle. Ce système d'échange s'appelle le partage de fichiers. Le pirate y dépose les logiciels, les films ou encore les musiques dont il a fait une copie afin de les distribuer partout dans le monde. De plus, les systèmes de partage de fichiers, dans une version plus récente, permettent l'échange des fichiers de façon anonyme, ce qui va compliquer la tâche des enquêteurs pour trouver le coupable et créer un manque à gagner pour les personnes bénéficiant d'une rémunération pour des droits d'auteurs. Par exemple, les musiques sont généralement protégées par les droits

[8] http://www.larousse.fr/dictionnaires/francais/num%C3%A9rique/55253

d'auteurs. Il est interdit de diffuser ces musiques sur internet sans l'accord préalable de son auteur. Comme l'auteur touche un pourcentage sur chaque album vendu, il aurait un manque à gagner si les clients téléchargent ces musiques gratuitement via le partage de fichiers.

Ensuite, nous avons les systèmes de droit numérique qui servent à limiter l'accès à certains fichiers ou fonctions de logiciel. Par exemple, les logiciels gratuits avec une version payante disponible grâce à une clé d'activation. Le pirate va simplement tenter de dénicher une clé d'activation valide afin de pouvoir se servir du logiciel sous sa version payante sans débourser le moindre centime.

Il existe plusieurs lois sur les atteintes liées à la propriété intellectuelle. Nous citerons, à titre d'exemple mais sans entrer dans les détails, la loi du15 mai 2007 relative à la répression de la contrefaçon et de la piraterie de droits de propriété intellectuelle et la loi du 30 juin 1994 relative aux droits d'auteur et aux droits voisins qui s'appliquent pour protéger les droits intellectuels sur le net.

4 LES INFRACTIONS SE RAPPORTANT AU CONTENU

Les infractions qui nous intéressent dans ce travail sont celles qui visent à sanctionner les contenus illicites présents sur internet. Ces infractions rassemblent notamment la pédopornographie, la haine raciale et la xénophobie, la calomnie, la diffamation, les jeux illégaux sur le net (que nous n'aborderons pas dans ce travail), le délit de presse sur internet et le cyberharcèlement. Mais avant de détailler les contenus illicites, nous allons vous expliquer la difficulté juridique principale qui empêche les États de lutter contre les contenus illicites: il s'agit du droit à la liberté d'expression.

CHAPITRE 3: LA GARANTIE DU DROIT À LA LIBERTÉ D'EXPRESSION

Le droit à la liberté d'expression fait partie des obstacles à la lutte contre la cybercriminalité, car il assure à tous le droit de ne pas être sanctionné pour ses opinions. La liberté d'expression doit être comprise au sens large. Elle inclut également la liberté de rechercher et d'obtenir des informations et la liberté de partager ses informations et ses idées. Il convient, dans la lutte contre la cybercriminalité, de garder un équilibre entre les intérêts de la répression des cybercriminels et le respect des droits fondamentaux.

1 SUR LE PLAN INTERNATIONAL

Au niveau du droit international, le droit à la liberté d'expression se retrouve principalement dans la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales:

> **Article 10 alinéa 1**: *"Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontière. Le présent article n'empêche pas les États de soumettre les entreprises de radiodiffusion, de cinéma ou de télévision à un régime d'autorisations".*

À la lecture de cet article, il semblerait, en principe, que les États ne puissent rien prévoir contre les contenus illicites. D'ailleurs, si les États n'ont pas la même législation en matière de contenu illicite, c'est parce que chaque État a une vision différente des limites du droit à la liberté d'expression, ce qui complique l'harmonisation des dispositions juridiques entre les États et l'établissement des sanctions pénales. Cependant, l'alinéa 2 présente les conditions où il est possible de passer outre le droit à la liberté d'expression et de punir les auteurs d'infractions:

Article 10 alinéa 2: *"L'exercice de ces libertés comportant des devoirs et des responsabilités peut être soumis à certaines formalités, conditions, restrictions ou sanctions prévues par la loi, qui constituent des mesures nécessaires, dans une société démocratique, à la sécurité nationale, à l'intégrité territoriale ou à la sûreté publique, à la défense de l'ordre et à la prévention du crime, à la protection de la santé ou de la morale, à la protection de la réputation ou des droits d'autrui, pour empêcher la divulgation d'informations confidentielles ou pour garantir l'autorité et l'impartialité du pouvoir judiciaire".*

Ce paragraphe nous explique sous quelles conditions il est possible de déroger au principe de liberté d'expression. Il faut noter que les États peuvent prévoir des sanctions contre les contenus illicites portant atteinte à la réputation d'une personne ou constituant un délit de droit pénal. Pour déroger au principe de la liberté d'expression, trois conditions doivent être prises en compte:

- l'exception doit être prévue dans la loi nationale,
- l'exception doit être une mesure nécessaire dans une société démocratique, c'est-à-dire, que la mesure existe pour garantir le respect des droits de chacun,
- cette mesure doit être légitime.

1.1 UNE RESTRICTION PRÉVUE PAR LA LOI

Selon la doctrine, *"l'immixtion dans l'exercice de la liberté d'expression doit être prévue par la loi, notion qui inclut non seulement le droit écrit mais également la jurisprudence. En outre, la loi doit à la fois être suffisamment accessible et prévisible, de manière à permettre aux individus de régler leur comportement en fonction d'une norme qu'ils ont effectivement la possibilité de connaître et qui présente un degré suffisant de précision"*[9].

[9] DOCQUIR, P.-F., "Contrôle des contenus sur Internet et liberté d'expression au sens de la Convention européenne des droits de l'homme", C.D.P.K., 2002, p. 173 à 193.

En d'autres termes, la loi doit être assez claire pour que les citoyens comprennent où se situe la limite entre le droit à la liberté d'expression et une infraction. De plus, cette restriction se rapproche de la notion de sécurité juridique puisqu'elle impose que le citoyen puisse savoir ce qui lui est permis et ce qui lui est interdit de faire.

Dans l'arrêt Sunday Times du 26 avril 1979, la CEDH ajoute la notion de "*loi suffisamment accessible*"[10]. Cela signifie que le citoyen doit être en mesure de déterminer comment la loi va s'appliquer dans un cas concret. Cet arrêt opposait le Royaume-Uni à Sunday Times, un journal de presse qui avait publié une série d'articles sur la thalidomide, une sorte de somnifère pris par les futures mamans, et ses effets néfastes sur les enfants. Cependant, comme le droit anglais disposait de principes contradictoires, la loi n'interdisait pas au journal de publier son article. La CEDH a déclaré qu'il y avait violation de la liberté d'expression.

1.2 UNE RESTRICTION INDISPENSABLE DANS UNE SOCIÉTÉ DÉMOCRATIQUE

La Cour européenne des droits de l'homme a dû interpréter cette condition pour en dégager deux éléments:

1.2.1 Un besoin social impérieux

Pour atteindre l'un des objectifs visés par la Convention, la mesure doit tout d'abord répondre à un besoin social impérieux. Il appartient aux législateurs nationaux de définir quels sont ces besoins sociaux impérieux qui justifient une restriction à la liberté d'expression. La CEDH examinera ensuite si les circonstances qui fondent le besoin social impérieux choisi par les autorités nationales sont assez convaincantes et utiles pour justifier d'une restriction à la prééminence du droit à la liberté d'expression.

[10] Cour eur. D. H., (6538/74) - Cour (Plénière) - Arrêt (au principal) - AFFAIRE SUNDAY TIMES contre. ROYAUME-UNI (N° 1) © Hudoc, 26/04/1979, (disponible sur http://hudoc.echr.coe.int/; consulté le 23 mars 2015).

Dans un arrêt de la CEDH du 21 janvier 1999[11], la Cour avait dû statuer sur le cas d'un journal satirique "*Le Canard enchaîné*" qui avait publié un article litigieux sur le patron de Peugeot. La CEDH a considéré qu'il y avait violation de la liberté d'expression puisque "*la "nécessité" d'une quelconque restriction à l'exercice de la liberté d'expression doit se trouver établie de manière convaincante. Certes, il revient en premier lieu aux autorités nationales d'évaluer s'il existe un "besoin social impérieux" susceptible de justifier cette restriction, exercice pour lequel elles bénéficient d'une certaine marge d'appréciation. Lorsqu'il y va de la presse, comme en l'espèce, le pouvoir d'appréciation national se heurte à l'intérêt de la société démocratique à assurer et à maintenir la liberté de la presse*"[12].

1.2.2 Le respect de la proportionnalité

Ensuite, la Cour a imposé le respect de la proportionnalité entre la restriction à la liberté d'expression et le but légitime poursuivi par le législateur, ce qui signifie que cette restriction doit être la moins attentatoire à la liberté d'expression et permettre d'atteindre l'objectif poursuivi par le législateur.

La CEDH, dans un arrêt du 3 octobre 2000[13], donne une illustration de l'application du principe de proportionnalité à la liberté d'expression. Dans les faits, monsieur Malaurie avait publié un article accusant un ancien dirigeant de la Sonacotra d'abuser de biens sociaux.

Monsieur Malaurie fut condamné par les juridictions françaises mais la CEDH estima que: "*la condamnation des journalistes ne représentait pas un moyen raisonnablement proportionné à la poursuite des buts légitimes visés, compte tenu de l'intérêt de la société démocratique à assurer et à maintenir la liberté de la presse*"[14]. La CEDH conclut qu'il y avait une violation de la liberté d'expression.

[11] Cour eur. D. H., Arrêt Fressoz et Roire contre France du 21 janvier 1999, n° 29183/95.
[12] Cour eur. D. H., Arrêt Fressoz et Roire contre France du 21 janvier 1999, n° 29183/95.
[13] Cour eur. D. H., Arrêt Roy et Malaurie contre France du 3 Octobre 2000, n° 34000/96.
[14] Cour eur. D. H., Arrêt Roy et Malaurie contre France du 3 Octobre 2000, n° 34000/96.

1.3 UNE RESTRICTION LÉGITIME

Cette condition signifie que l'ingérence de l'autorité doit avoir comme objectif l'un des buts visés par l'article 10 alinéa 2 de la Convention des droits de l'homme, par exemple, la protection de la réputation ou encore la protection des droits d'autrui. Si le législateur poursuit un autre objectif que ceux visés par la Convention, le droit à la liberté d'expression s'appliquera.

Dans un arrêt de la CEDH[15], la Cour a statué sur le cas de deux journalistes qui avaient diffamé des juges autrichiens dans un article. Les journalistes ont été condamnés et la CEDH a jugé que cette condamnation se justifiait pour protéger les droits d'autrui. En effet "*Il convient cependant de tenir compte de la mission particulière du pouvoir judiciaire dans la société. Comme garant de la justice, valeur fondamentale dans un Etat de droit, son action a besoin de la confiance des citoyens pour prospérer. Aussi peut-il s'avérer nécessaire de protéger celle-ci contre des attaques destructrices dénuées de fondement sérieux, alors surtout que le devoir de réserve interdit aux magistrats visés de réagir*"[16]. En résumé, cette restriction de la liberté d'expression était légitime pour protéger les droits du pouvoir judiciaire et pour garder la confiance des citoyens.

2 SUR LE PLAN NATIONAL

Au niveau du droit belge, l'article 19 de la Constitution garantit le droit à la liberté d'expression.

> **Article 19**: *"La liberté des cultes, celle de leur exercice public, ainsi que la liberté de manifester ses opinions en toute matière, sont garanties, sauf la répression des délits commis à l'occasion de l'usage de ces libertés".*

Cet article n'est que le parallèle en droit belge de l'article 10 de la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales.

[15] Cour eur. D. H., Arrêt Prager et Oberschlick contre Autriche du 26 avril 1995, série A n° 313, p. 18, § 37, p. 19, § 38
[16] Cour eur. D. H., Arrêt Prager et Oberschlick contre Autriche du 26 avril 1995, série A n° 313, p. 18, § 37, p. 19, § 38

CHAPITRE 4: LES CONTENUS ILLICITES

Après avoir identifié quelles sont les infractions relatives à la cybercriminalité, ainsi que la portée du droit à la liberté d'expression, il convient de définir ce que sont les contenus illicites sur internet. Pour la plupart des infractions, le web n'est qu'un moyen qui facilite la commission de l'infraction. D'ailleurs, ces infractions existaient déjà dans le Code pénal belge. Cependant, l'apparition de nouvelles technologies a obligé les législateurs européens et nationaux à prendre de nouvelles normes et les magistrats belges ont dû interpréter les lois existantes pour les appliquer aux délits commis par le biais d'internet.

Avant tout, il n'existe pas de définition légale d'un contenu illicite mais les praticiens du droit en ont donné une définition. Celle-ci vient d'un mémoire sur la pédopornographie:

> *"Un contenu illicite est un contenu interdit à l'ensemble de la population, quel que soit l'âge des destinataires éventuels et quel que soit le support. Il s'agit d'un contenu pour lequel la société s'accorde à dire qu'il est contraire à la dignité humaine. Cette catégorie de contenu englobe entre autres la pédopornographie, les formes extrêmes de violence, l'incitation à la haine, à la discrimination raciale ou à la violence"*[17].

Les contenus illicites apparaissent surtout sur le "darknet" car ils sont retirés des moteurs de recherche traditionnels. Qu'est-ce que le "darknet"? Cette question me permet d'expliquer l'image de la page de garde de ce travail[18]. Le "darknet" ou le web profond est la partie cachée d'internet où il est possible de naviguer sur le net dans l'anonymat le plus total. La première caractéristique du web profond est qu'il n'est pas accessible par les moteurs de recherche traditionnels tels que Firefox ou Google chrome. Il faut pour cela utiliser le navigateur Tor[19] pour

[17] V. KAISER, "La protection des mineurs sur Internet: la problématique de la pédopornographie et des contenus jugés préjudiciables", 2010.
Livre vert de la Commission du 16 octobre 1996 sur la protection des mineurs et de la dignité humaine dans les services audiovisuels et d'information, C.O.M. (96) 483 final, p. 7.
[18] Voir annexe n° 3
[19] Voir annexe n° 4

accéder aux pages qui finissent en ".onion". Mais avant de parler des dispositions pénales,
il faut savoir quel État est compétent pour juger d'un contenu illicite.

1 JURIDICTION COMPÉTENTE

En matière de cybercriminalité, les éléments constitutifs de l'infraction se réalisent rarement exclusivement sur le sol belge. Par exemple, un pirate peut poster des contenus illicites sur un ordinateur situé en France et ces contenus seront visibles en Belgique. Le grand principe en matière de compétence territoriale est repris par l'article 3 du Code pénal:

> ***Article 3****: "L'infraction commise sur le territoire du royaume, par des Belges ou par des étrangers, est punie conformément aux dispositions des lois belges. "*

À la lumière de cet article, on comprend que la loi et la juridiction compétente sont celles du lieu où se commet l'infraction. Mais comme les éléments constitutifs de l'infraction peuvent être réunis sur plusieurs territoires, quand peut-on considérer que le lieu de l'infraction est le territoire belge? La théorie objective de l'ubiquité permet de répondre à cette question. Cette théorie est née de la jurisprudence belge. Voici ce que la doctrine dit sur la théorie de l'ubiquité:

> *"L'infraction est réputée commise sur le territoire d'un État dès lors qu'un des faits constitutifs a eu lieu sur ce territoire. En matière de presse, la publicité est sans aucun doute un élément constitutif et même la caractéristique essentielle des infractions prévues et réprimées par la loi. Par conséquent, les infractions sont réputées commises partout où l'information publiée peut être reçue ou entendue"*[20].

Il suffit qu'un des éléments constitutifs de l'infraction se situe sur le territoire belge pour que les juridictions belges soient compétentes et qu'elles appliquent le droit

[20] VALCKE, P., UYTTENDAELE, C., "Racisme et négationnisme sur l'Internet: les affaires Infonie et Yahoo! Bis", R.D.T.I., 2002/2, p. 87.

belge et européen. Le droit belge s'applique puisque les dispositions pénales sont d'ordre public.

Notons aussi cette particularité lorsqu'il s'agit d'un délit de presse: puisque la publicité est un élément constitutif du délit de presse, n'importe quelle juridiction belge pourrait être compétente dès que, sur le territoire de sa juridiction, elle peut recevoir ou entendre l'information publiée. Par exemple, un délit de presse à caractère raciste visible partout en Belgique pourrait être jugé par le tribunal correctionnel de Gand, de Bruxelles ou encore celui de Liège. Nous reviendrons sur le délit de presse plus loin dans ce travail. (Chapitre 4, sous-section 3.4)

2 LES CONTENUS ILLICITES DANS LE DROIT EUROPÉEN

La Convention sur la cybercriminalité[21] signée à Budapest le 23 novembre 2001 ci-après dénommée "Convention sur la cybercriminalité" ne prévoit que des dispositions pour réprimer la pédopornographie. Elle ne sanctionne rien d'autre à cause des États-Unis où la liberté d'expression figure dans le premier amendement de leur Constitution. Pour les États-Unis, la liberté d'expression n'a que peu de limites, raison pour laquelle la Convention sur la cybercriminalité ne sanctionne pas le racisme et la xénophobie. La Convention sur la cybercriminalité a déjà été signée par quarante-neuf États membres ou non membres du Conseil de l'Europe et ratifiée par quarante-cinq États[22]. Bien que cette Convention ait été adoptée par le Conseil de l'Europe, elle est ouverte aux autres États en vue d'une coopération internationale dans la lutte contre la cybercriminalité.

Pour remédier à cette situation, il existe un protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques. Mais la Belgique n'a pas jugé utile de ratifier le protocole, car sa législation incrimine déjà le racisme et la xénophobie que nous développerons plus loin. (Chapitre 4, sous-section 3.5).

[21] Convention sur la cybercriminalité signée à Budapest le 23 novembre 2001 et approuvée par la loi du 20 août 2012 (Disponible sur http://www.conventions.coe.int/Treaty/fr/Treaties/Html/185.htm; page consulté le 15 juillet 2014).
[22] Voir annexe n° 5

En revanche, trente-huit États ont signé le protocole et seulement vingt-quatre États l'ont ratifié[23].

2.1 LA PÉDOPORNOGRAPHIE AU NIVEAU EUROPÉEN

La Convention sur la cybercriminalité donne une définition de la pornographie enfantine dans son article 9 §2. Il s'agit de *" toute matière pornographique représentant de manière visuelle un mineur se livrant à un comportement sexuellement explicite; une personne qui apparaît comme un mineur se livrant à un comportement sexuellement explicite; des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite".* La Convention sur la cybercriminalité évoque les lignes directrices que les États doivent suivre pour punir la pédopornographie sur la toile:

> **Article 9 §1**: *"Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les comportements suivants lorsqu'ils sont commis intentionnellement et sans droit:*
>
> - *La production de pornographie enfantine en vue de sa diffusion par le biais d'un système informatique;*
> - *L'offre ou la mise à disposition de pornographie enfantine par le biais d'un système informatique;*
> - *La diffusion ou la transmission de pornographie enfantine par le biais d'un système informatique;*
> - *Le fait de se procurer ou de procurer à autrui de la pornographie enfantine par le biais d'un système informatique;*
> - *La possession de pornographie enfantine dans un système informatique ou un moyen de stockage de données informatiques".*

[23] Voir annexe n° 6

Au terme de cet article, on constate que le producteur qui diffuse de la pédopornographie sur la toile et le simple consommateur doivent être punis par les États. Nous verrons au niveau national que la Belgique a bien suivi la Convention sur la cybercriminalité.

Le paragraphe 3 de l'article 9 concerne l'âge des personnes représentées. Mais l'âge auquel les enfants atteignent la majorité varie d'un État à l'autre. Il a été décidé que "le terme mineur désigne toute personne âgée de moins de 18 ans". Mais les États peuvent abaisser cette limite jusqu'à 16 ans.

> *"Aux fins du paragraphe 2, le terme «mineur» désigne toute personne âgée de moins de 18 ans. Une Partie peut toutefois exiger une limite d'âge inférieure, qui doit être au minimum de 16 ans".*

3 LES CONTENUS ILLICITES EN DROIT BELGE

3.1 LA PÉDOPORNOGRAPHIE

Il s'agit sans doute de l'infraction la plus connue sur internet. La pédopornographie se définit par la représentation d'un ou plusieurs enfants impliqués dans des activités sexuelles. En Belgique, la diffusion sur la toile ainsi que la possession de pédopornographie sont punissables pénalement.

3.1.1 La diffusion de pornographie enfantine

La diffusion de pédopornographie est prévue dans l'article 383bis §1 du Code pénal:

> **Article 383bis §1**: *"Sans préjudice de l'application des articles 379 et 380, quiconque aura exposé, vendu, loué, distribué, diffusé ou remis des emblèmes, objets, films, photos, diapositives ou autres supports visuels qui représentent des positions ou des actes sexuels à caractère pornographique, impliquant ou présentant des mineurs ou les aura, en vue du commerce ou de la distribution, fabriqués ou détenus, importés ou fait im-*

porter, remis à un agent de transport ou de distribution, sera puni de la réclusion de cinq ans à dix ans et d'une amende de cinq cents [euros] à dix mille [euros]".

Dans cet article, l'élément matériel est le suivant, le prévenu doit avoir diffusé des images pornographiques représentant des mineurs d'âge. En ce qui concerne l'application de l'article 383bis §1 du Code pénal sur internet, la Cour de cassation a jugé que le terme "diffuser" ou "exposer" vise également les hyperliens vers un site web à caractère pornographique et représentant des mineurs d'âge[24]. Dès lors, nous pouvons considérer que le terme "diffuser" permet de sanctionner la pédopornographie sur internet. Quant à l'élément moral, il s'agit d'un dol général.

3.1.2 La simple possession/consultation de matériel pédopornographique

Pour savoir quand la possession de matériel pédopornographique est établie, il faut regarder le cas d'espèce mais E. Wery souligne que deux écoles s'affrontent pour déterminer la limite de cette possession. "*D'une part, ceux pour qui le principe d'interprétation restrictive du droit pénal doit primer: on ne peut pas élargir la portée de l'article par une interprétation téléologique*[25]*. D'autre part, ceux pour qui la volonté du législateur est de combattre la possession de façon absolue au nom de l'intérêt supérieur de la défense des mineurs"*[26]*.* Lorsque l'on analyse l'article 383bis §2 du Code pénal, on s'aperçoit que le législateur privilégie la seconde école, son objectif étant de punir les simples consommateurs.

> **Article 383bis §2**: *"Quiconque aura sciemment possédé les emblèmes, objets, films, photos, diapositives ou autres supports visuels visés sous le § 1er [ou y aura, en connaissance de cause, accédé par un système in-*

[24] Cass., 3 février 2004, n° F-20040203-3, inédit (disponible sur www.juridat.be; consulté le 27 octobre 2014).
[25] Une interprétation téléologique consiste à rechercher le but du législateur quand il a pris une norme.
[26] Wery, E., "La visualisation de pornographie enfantine est-elle punissable?", *Droit & technologie*, le 1er août 2011 [en ligne]. (Disponible sur: http://www.droit-technologie.org/actuality-1422/la-visualisation-de-pornographie-enfantine-est-elle-punissable.html; consulté le 21 juillet 2014).

formatique ou par tout moyen technologique], sera puni d'un emprisonnement d'un mois à un an et d'une amende de cent [euros] à mille [euros]".

Puisque l'article vise les "autres supports visuels visés sous le §1er" et que la Cour de cassation considère que le terme "diffuser" permet de sanctionner la pédopornographie sur internet, cet article 383bis §2 s'applique aussi au simple consommateur sur la toile.

Ici, nous analyserons les éléments constitutifs de l'infraction de la possession et de la consultation de pédopornographie.

3.1.2.1 La possession de pédopornographie

L'élément matériel est la possession de matériel pédopornographique. Cette possession ne nécessite pas de lien de propriété entre le consommateur et le matériel pédopornographique. Par exemple, le fait de posséder des images pédopornographiques sur un format papier, sur un CD-Rom ou un disque dur est considéré comme une possession.

En plus de la possession, un élément moral est requis. L'auteur doit avoir "sciemment" possédé ces images. Ce terme est utilisé pour éviter que des personnes consultant de la pornographie sans savoir que les acteurs sont mineurs soient sanctionnées par cet article. L'intention du possesseur de commettre l'acte interdit de possession de pornographie représentant des mineurs est l'élément moral de l'article 383bis §2. Il devait avoir conscience qu'il commettait une infraction. Donc, s'il est prouvé que l'auteur des faits a possédé des images en sachant que les acteurs étaient des mineurs d'âge, il pourra être condamné.

3.1.2.2 La consultation de pédopornographie

L'autre possibilité est la simple consultation par un moyen technologique, par exemple, via un matériel informatique. La consultation d'un site internet contenant de la pédopornographie est l'élément matériel de l'infraction. Quant à l'élément moral, cette personne aura accédé à la pédopornographie en toute connais-

sance de cause. L'internaute devait savoir que le site sur lequel il accédait montrait des mineurs se livrant à des actes sexuels.

Voici un exemple précis de consultation de matériel pédopornographique dans un arrêt de la Cour de cassation rendu le 20 avril 2011.

3.1.3 Jurisprudence

Tout d'abord, voici les faits qui ont été présentés à la Cour de cassation[27]: le prévenu était accusé d'avoir consulté sur un site informatique des vidéos pornographiques impliquant des mineurs. Dans un arrêt rendu par la Cour d'appel de Liège le 23 novembre 2010, le prévenu avait été condamné sur base de l'article 383bis §2 du Code pénal.

Ensuite, la position du demandeur était la suivante: il soutenait que l'arrêt rendu par la Cour d'appel de Liège violait l'article 383bis du Code pénal puisque cet arrêt donne une interprétation par analogie[28], en ce que l'arrêt avait considéré que la possession ne requérait pas que l'utilisateur télécharge ou imprime l'image, ni que l'utilisateur doive la détenir de manière continue. Alors que, selon le demandeur, les articles du Code pénal sont de stricte interprétation[29].

Il faut en conclure pour le demandeur que la possession de ces images sur un ordinateur impliquait un téléchargement ou une impression de ces images et, par conséquent, que le demandeur détenait ces images en continu sur support informatique ou papier.

Mais selon le raisonnement de la Cour de cassation, il ressort des travaux préparatoires que la loi a pour objectif la protection des mineurs et que la condamnation du simple consommateur est possible pour lutter contre la pédopornographie.

Contrairement aux assertions du demandeur, le seul fait d'accéder à un site internet afin de consulter ces images en sachant qu'elles présentent un caractère pé-

[27] Cass., (2ème ch.), 20 avril 2011, P.10.2006.F, R.D.T.I., 2011/3, n° 44, p. 27-28.
[28] Interprétation par analogie: elle consiste à étendre l'application d'une règle de droit à une situation voisine.
[29] Stricte interprétation: le juge doit s'en tenir au texte.

dopornographique suffit, car cette consultation signifie que le demandeur a été en possession d'un ordinateur montrant des images pédopornographiques.

De plus, le demandeur avait détenu l'adresse du site et y a posté des messages indiquant qu'il savait qu'il consultait un site dont le contenu présentait un caractère sexuel et interdit.

Par ces motifs, la Cour de cassation a rejeté le pourvoi.

Nous pouvons en conclure que la possession d'une image pédopornographique ne requiert pas que l'utilisateur possède l'image de manière continue. La simple consultation suffit pour être condamné si l'utilisateur accède à de la pédopornographie en toute connaissance de cause. Dès que ces conditions sont remplies, nous pouvons considérer que l'article 383 bis §2 du Code pénal s'applique.

3.2 LA DIFFAMATION ET LA CALOMNIE

3.2.1 Distinction entre la diffamation et la calomnie

Dans un premier temps, il convient de faire la distinction entre la diffamation et la calomnie. La différence entre ces deux notions se situe dans le Code pénal:

> **Article 443 alinéa 1**: *"Celui qui, dans les cas ci-après indiqués, a méchamment imputé à une personne un fait précis qui est de nature à porter atteinte à l'honneur de cette personne ou à l'exposer au mépris public, et dont la preuve légale n'est pas rapportée, est coupable de calomnie lorsque la loi admet la preuve du fait imputé, et de diffamation lorsque la loi n'admet pas cette preuve".*

La différence entre la diffamation et la calomnie se situe au niveau de la possibilité de rapporter la preuve des faits imputés. Dans la calomnie, l'auteur des propos calomnieux peut apporter la preuve des faits qu'il reproche à la victime car la loi l'y autorise mais il reste incapable de prouver que les faits reprochés sont vrais. Cependant, si l'auteur prouve que les faits reprochés sont vrais, il ne sera pas poursuivi.

Alors que dans la diffamation, la loi ne permet pas à l'auteur de rapporter la preuve des faits imputés à la victime, soit parce qu'il y a prescription des faits reprochés, soit parce ces faits font partie de la vie privée de la victime et sont protégés par l'article 8 de la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales. L'auteur ne pourra pas utiliser les faits reprochés, même s'ils sont vrais pour se défendre car comme la loi n'admet pas la preuve du fait imputé; la preuve légale n'est jamais rapportée.

3.2.2 Éléments constitutifs communs de la diffamation et de la calomnie

3.2.2.1 La publicité

Cet article nous donne les différents cas dans lesquels on peut parler de diffamation et de calomnie. Les deux derniers cas donnés par l'article 444 du Code pénal concernent le net.

> **Article 444**: *"Le coupable sera puni d'un emprisonnement de huit jours à un an et d'une amende de vingt-six [euros] à deux cents [euros], lorsque les imputations auront été faites:*
>
> - *Soit dans des réunions ou lieux publics;*
> - *Soit en présence de plusieurs individus, dans un lieu non public, mais ouvert à un certain nombre de personnes ayant le droit de s'y assembler ou de le fréquenter;*
> - *Soit dans un lieu quelconque, en présence de la personne offensée et devant témoins;*
> - *Soit par des écrits imprimés ou non, des images ou des emblèmes affichés, distribués ou vendus, mis en vente ou exposés aux regards du public;*
> - *Soit enfin par des écrits non rendus publics, mais adressés ou communiqués à plusieurs personnes".*

Nous pouvons noter que la première condition pour être en présence d'une diffamation ou d'une calomnie est la publicité. Sur le net, la doctrine considère que "*les propos diffamants ou injurieux sur l'Internet, seront le plus souvent diffusés par écrit et donc considérés comme publics puisque la condition de publicité est remplie dès que les propos sont adressés à plus d'un seul destinataire, ce qui sera a priori toujours le cas lors d'une diffusion sur un site web ou un réseau social*"[30]. À titre d'exemple, notons la diffusion par blog où les messages postés sur un forum de discussion entrent clairement dans le champ d'application de l'article 444 du Code pénal.

De plus, la publicité doit être réelle et effective, ce qui implique la présence d'un public et la communication d'un message à ce public.

3.2.2.2 L'imputation à une personne d'un fait précis

L'élément matériel de la diffamation et de la calomnie est l'imputation d'un fait précis à une personne, en d'autres mots, attribuer à une personne des paroles ou une attitude. La précision du fait sera analysée par le juge de fond. S'il estime que le fait reproché est assez précis, l'infraction sera qualifiée de calomnie ou de diffamation; sinon, elle sera considérée comme une injure.

Ensuite, la personne à qui l'on reproche un fait doit être identifiable. Il n'est pas indispensable que la personne soit citée par son nom ou prénom. Il suffit que les tiers ou la personne visée puissent reconnaitre de qui il s'agit.

3.2.2.3 L'intention méchante

Il s'agit de l'élément moral. Ici, c'est un dol spécial où il est nécessaire de rechercher l'intention particulière de l'auteur en plus de sa conscience à commettre une infraction. Dans ce cas-ci, il faut que la victime prouve que l'auteur avait la volonté de nuire ou de l'offenser.

[30] CASSART, A., "L'extension de la notion de communauté d'intérêts aux réseaux sociaux", R.D.T.I., 2013/3, n° 52, p. 101-106.

3.2.2.4 *Un fait de nature à porter atteinte à l'honneur de la personne ou à l'exposer au mépris public*

Il appartient au juge de fond d'examiner si le fait reproché porte atteinte à l'honneur ou expose la victime au mépris public. Comme c'est une question de fait, nous allons voir dans le référé qui suit un cas concret où le juge a dû examiner les messages litigieux et déterminer s'ils portent atteinte à l'honneur de la victime.

3.2.3 Référé du tribunal civil de Bruxelles

Le tribunal civil de Bruxelles a statué en référé le 2 mars 2000 sur une affaire de calomnie sur un forum de discussion[31].

Dans les faits, le demandeur est député à la Région de Bruxelles-capitale. Le défendeur est un politologue qui a écrit des propos jugés diffamatoires par le demandeur sur un forum de discussion. Quant au second défendeur, il s'agit de la s. a. Belgacom Skynet qui possède le serveur où sont hébergés les propos litigieux.

Le raisonnement du tribunal est le suivant: il admet que la diffusion de messages sur la toile est considérée comme une communication publique si le contenu du message est accessible rien qu'en composant l'adresse du site sans autre condition pour y accéder. L'article 444 du Code pénal l'indique également dans le cas où des écrits "imprimés ou non, des images ou des emblèmes affichés, distribués ou vendus, sont mis en vente ou exposés aux regards du public". Cette condition est remplie puisque le site est ouvert à tous.

Ensuite, le tribunal rappelle que la calomnie ou la diffamation nécessite une intention méchante. Sinon, il s'agit d'un quasi-délit, à condition que la victime prouve qu'elle a subi un dommage et que l'auteur a commis une faute en lien causal avec ce dommage (voir article 1382 du Code civil).

Dans le cas d'espèce, le tribunal a dû vérifier chaque message pour apprécier le caractère fautif, calomnieux ou diffamatoire. Nous ne comptons pas examiner

[31] Civ. Bruxelles (réf.), 2 mars 2000, J.T., 2002/6, n° 6042, p. 113-116.

tous les messages. Nous allons en choisir deux où le raisonnement du tribunal est différent. Commençons par le quatrième message du 1 juillet 1999:

> *"A Montréal, il y a quelqu'un qui a eu l'honneur " de rencontrer O... à Bruxelles, et qui a pu assez rapidement se faire une idée du personnage et de la haute opinion qu'il a de ses compatriotes émigrés: c'est A... K..., Maghreb Observateur. O... lui avait notamment dit (en ma présence) que les Marocains d'ici ne lisent pas de journaux; à part les suppléments sportifs... "*

Dans ce message, bien que la critique soit virulente, le tribunal a estimé que le défendeur n'avait pas dépassé les limites de la liberté d'expression. En conséquence, le message ne sera pas retiré du forum de discussion.

Par contre, Le cinquième message du 4 septembre 1999 rapporte:

> *"... ce O... est un pion du Maghzen en Belgique et sa duplicité n'a pas de limites. Personnellement, j'estime qu'il constitue carrément un risque pour la Belgique sur le plan de la sûreté de l'État ...".*

Ce message affirme que le demandeur a rejoint le Maghzen. Pour le tribunal, le défenseur a outrepassé les limites de la liberté d'expression car affirmer que le demandeur est un pion du Maghzen n'est pas l'expression d'une opinion mais bien l'imputation d'un fait dont il ne peut peut-être pas rapporter la preuve. Dans ce cas présent, le tribunal va ordonner le retrait de ce message du forum de discussion.

3.3 LE CYBERHARCÈLEMENT

La multiplication des profils sur les réseaux sociaux a engendré un nouveau moyen afin de harceler les gens sur le net. Cette pratique se nomme le cyberharcèlement et touche majoritairement les adolescents.

Avant de parler de cyberharcèlement, il faut définir ce qu'est le harcèlement. Le dictionnaire Larousse définit le harcèlement comme étant le fait de: "Soumettre

quelqu'un à de continuelles pressions, sollicitations"[32]. Mais le cyberharcèlement n'a pas de définition à proprement parler car il en existe une multitude. Toutefois, la doctrine en a donné une définition:

> *"Il s'agit de l'utilisation des technologies de l'information et de la communication (comme l'e-mail, le GSM et les sms, la messagerie instantanée, les pages Web personnelles) pour adopter délibérément, répétitivement et de manière agressive un comportement à l'égard d'un individu ou d'un groupe avec l'intention de provoquer un dommage à autrui"[33].*

En tout cas, le cyberharcèlement nécessite l'utilisation d'un moyen de communication électronique. Cette notion regroupe le harcèlement par téléphone ou sur les réseaux sociaux.

La Belgique n'a jamais pris de disposition légale supplémentaire pour lutter contre ce nouveau phénomène. Il existe deux articles qui permettent de punir le cyberharcèlement, tout d'abord, l'article 442bis du Code pénal:

> **Article 442bis alinéa 1er**: *"Quiconque aura harcelé une personne alors qu'il savait ou aurait dû savoir qu'il affecterait gravement par ce comportement la tranquillité de la personne visée, sera puni d'une peine d'emprisonnement de quinze jours à deux ans et d'une amende de cinquante [euros] à trois cents [euros], ou de l'une de ces peines seulement".*

3.3.1 Les éléments constitutifs du harcèlement prévus à l'article 442bis du Code pénal

3.3.1.1 Le dépôt d'une plainte par la victime

> **Article 442bis alinéa 3**: *"Le délit prévu par le présent article ne pourra être poursuivi que sur la plainte de la personne qui se prétend harcelée".*

[32] http://www.larousse.fr/dictionnaires/francais/_harceler/39062
[33] DEMOULIN Marie, HEIRMAN Wannes, VAN DER PERRE Aurélie, WALRAVE Michel, "Cyberharcèlement: risque du virtuel, impact dans le réel", internet-observatory.be.

Le dépôt de plainte différencie l'article 442bis du Code pénal de l'article 145 §3bis de la loi du 13 juin 2005 relative aux communications électroniques. Cet élément constitutif de l'infraction est nécessaire parce que le juge pourra prendre en compte les sentiments de la victime.

3.3.1.2 Les éléments matériels

Tout d'abord, il faut un comportement harcelant de l'auteur envers une personne déterminée. Il n'existe pas de définition légale du harcèlement afin de pouvoir sanctionner un maximum de comportements. Ensuite, il faut une atteinte à la tranquillité de la personne. Pour finir, il faut un lien de cause à effet entre le comportement du harceleur et l'atteinte à la tranquillité de la victime.

3.3.1.3 L'élément moral

L'auteur du harcèlement, en plus d'avoir la conscience qu'il commettait une infraction, savait ou devait savoir qu'il importunait la victime. Ce dol spécial exige que l'harceleur ait connaissance que son comportement avait des conséquences néfastes pour la victime.

Il faut noter que l'on se place au niveau de la victime pour déterminer le caractère harcelant de l'attitude du harceleur et son impact sur la victime. C'est sur base de cet élément moral que la plainte de la victime est indispensable pour engager les poursuites.

3.3.2 Les éléments constitutifs du harcèlement prévus à l'article 145 §3bis de la loi du 13 juin 2005 relative aux communications électroniques

Le deuxième article qui permet de punir le cyberharcèlement est l'article 145 §3bis de la loi du 13 juin 2005 relative aux communications électroniques[34] qui prévoit une sanction dont le champ d'application se rapproche de celui de l'article 442bis du Code pénal et qui s'applique dès que l'auteur des faits utilise un moyen de communication électronique:

[34] L. du 13 juin 2005 relative aux communications électroniques. Art. 145. §3bis, M.B., le 20 juin 2005, p. 28070.

Article 145 §3bis: *"Est punie d'une amende de 20 EUR à 300 EUR et d'un emprisonnement de quinze jours à deux ans ou d'une de ces peines seulement la personne qui utilise un réseau ou un service de communications électroniques ou d'autres moyens de communication électronique afin d'importuner son correspondant ou de provoquer des dommages".*

3.3.2.1 Importuner son correspondant

Cette condition est très simple à comprendre, il suffit que l'auteur importune son correspondant. Par exemple, des appels téléphoniques répétés tard dans la soirée, non sollicités par la victime, peuvent être une manière d'importuner autrui.

3.3.2.2 L'utilisation d'un moyen de communication électronique

Aujourd'hui, les moyens de communication électronique se sont multipliés. Ainsi, le fait d'utiliser un téléphone, un e-mail, un réseau social, un logiciel de messagerie instantanée, ou tout autre moyen informatique est considéré comme un moyen de communication électronique au sens de l'article 145 §3bis.

3.3.2.3 L'élément moral

Il s'agit d'un dol général, l'auteur devait avoir la volonté d'importuner son correspondant.

3.3.3 Comparaison entre l'article 442bis du Code pénal et l'article 145 §3bis de la loi du 13 juin 2005 relative aux communications électroniques

Notons que la peine encourue est la même sauf en ce qui concerne le minimum de l'amende qui est de 50 € pour l'article 442 bis du Code pénal et 20 € pour l'article 145 §3bis de la loi du 13 juin 2005. En revanche, la simple utilisation d'un moyen électronique pour harceler le correspondant suffit pour être sanctionné par cette loi.

La différence majeure entre ces deux dispositions se situe au niveau du dépôt de la plainte. Un dépôt de plainte est requis pour poursuivre le harceleur sur pied de

l'article 442bis du Code pénal, alors que cette condition n'existe pas dans l'article 145 §3bis.

Une question préjudicielle a été posée à la Cour constitutionnelle[35] afin de déterminer si l'article 145 §3bis ne violait pas les articles 10 et 11 de la Constitution à cause de l'absence du dépôt de plainte comme condition de recevabilité des poursuites. Mais la Cour constitutionnelle a estimé que, même si les champs d'application sont les mêmes, les éléments constitutifs étant différents, il n'y a pas violation des articles 10 et 11 de la Constitution.

Le principal avantage de l'article 145 §3bis par rapport à l'article 442bis du Code pénal réside dans l'élément matériel de ces infractions. Il y a moins d'éléments matériels à prouver. Ensuite, il faut prouver que l'auteur a la conscience de commettre une infraction. Mais il n'est pas nécessaire de démontrer une intention particulière dans l'article 145 §3bis, contrairement à l'article 442bis où il faut prouver que le harceleur a la connaissance que son comportement affecte la tranquillité de la victime.

3.3.4 Jurisprudence

La Cour de cassation[36] s'est prononcée sur un cas de cyberharcèlement dans un arrêt du 29 octobre 2013.

Les faits étaient les suivants: le demandeur était condamné pour harcèlement par un arrêt rendu le 6 juin 2013 par la Cour d'appel d'Anvers, chambre correctionnelle. Il avait posté pendant cinq jours une vidéo contenant des propos discriminatoires à l'égard d'un groupe de non-musulmans sur le site de YouTube, ce qui a eu pour conséquence des insultes portant atteinte à la tranquillité du défendeur dans les commentaires.

La position du demandeur était la suivante: il invoquait une violation de l'article 442bis du Code pénal puisqu'il n'a posé qu'un seul acte, celui de poster la vidéo

[35] C.C., 22 décembre 2011, n° 198/2011, © Cour constitutionnelle de Belgique, 25/04/2012, (disponible sur www.const-court.be; consulté le 15 mars 2015).

[36] Cass., (2ème ch.), 29 octobre 2013, J.T.,2014/21, n° 6565, p. 391-392.

sur le net. Or, le harcèlement devant présenter un caractère répétitif, le demandeur ne devait pas être condamné.

Un autre moyen important invoqué par le demandeur est la violation de l'article 10 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales et 19 de la Constitution. Selon le demandeur, ses propos et son film ne peuvent être sanctionnés car ils n'ont pas incité à la discrimination; or, il faudrait prouver l'incitation pour être sanctionné.

Cependant, le raisonnement de la Cour est différent. Elle a décidé que le harcèlement nécessite des comportements continus et incessants. En postant une vidéo sur YouTube, les insultes dans les commentaires qui ont suivis présentaient un caractère quasi-permanent. De plus, la vidéo, diffusée sur internet, a pu être vue par toute personne dans le monde pendant cinq jours et les commentaires visibles de manière permanente. Dès lors, le demandeur avait l'intention d'affecter la tranquillité du défendeur étant donné qu'il a choisi le média le plus adéquat.

Quant à la violation de l'article 10 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales et 19 de la Constitution, la Cour a décidé que, compte tenu du contenu, du ton et du caractère répétitif, le demandeur incite intentionnellement à la discrimination. Alors, la Cour de cassation a rejeté le pourvoi.

Nous pouvons en conclure que la Cour de cassation a considéré que le seul agissement du prévenu était incessant et donc constitutif du harcèlement car les messages et la vidéo sont restés visibles en permanence et que cet agissement présentait un caractère continu puisque la vidéo est restée en ligne durant cinq jours.

3.4 LES CONTENUS ILLICITES PAR VOIE DE PRESSE

3.4.1 La juridiction compétente en matière de délit de presse

En Belgique, deux juridictions peuvent être amenées à statuer sur le délit de presse: il s'agit de la cour d'assises et du tribunal correctionnel. L'article 150 de la Constitution permet de déterminer quelle juridiction est compétente.

> ***Article 150*** *"Le jury est établi en toutes matières criminelles et pour les délits politiques et de presse [, à l'exception des délits de presse inspirés par le racisme ou la xénophobie]".*

À la lecture de cet article, le délit de presse est du ressort de la cour d'assises sauf si le délit de presse vise un acte à caractère racisme ou xénophobe. Dans ce cas, le délit de presse est du ressort du tribunal correctionnel.

3.4.2 La protection du constituant de la presse écrite

> **Article 25 de la Constitution***: "La presse est libre; la censure ne pourra jamais être établie; il ne peut être exigé de cautionnement des écrivains, éditeurs ou imprimeurs.*
>
> *"Lorsque l'auteur est connu et domicilié en Belgique, l'éditeur, l'imprimeur ou le distributeur ne peut être poursuivi".*

Il faut d'abord noter que le constituant ne donne pas de définition de la notion de presse. Ensuite, cet article interdit la censure ainsi que le cautionnement et institue la responsabilité en cascade, à condition que l'auteur ne soit pas connu et domicilié en Belgique.

3.4.3 Les conditions d'un délit de presse sur internet

Il n'existe aucun article qui donne les conditions du délit de presse. La Cour de cassation a alors défini plusieurs conditions dans sa jurisprudence que la doctrine a rassemblé. "*Plusieurs conditions doivent être réunies pour qu'une infraction soit qualifiée de délit de presse, à savoir une infraction de droit commun commise par voie de presse, un élément intellectuel (manifestation d'une pensée, expression d'une opinion abusive ou illicite, abus de la liberté d'expression) et un élément matériel (écrit imprimé, reproduit et publié)*"[37].

[37] DONY, C., "La presse, une notion que le Constituant tarde à (re)définir ...", J.L.M.B., 2010/3, p. 137-142.

3.4.3.1 Un délit de droit commun

Ce délit de droit commun doit être réalisé par voie de presse. Les délits de droit commun regroupent des délits tels que la calomnie, la diffamation, l'injure, le racisme et la xénophobie, etc.

Par voie de presse, il faut comprendre que l'opinion litigeuse se trouve dans un texte imprimé qui a vocation d'être reproduit et publié comme, par exemple, un journal de presse. Il a été admis par la Cour de cassation[38] que le délit de presse peut être commis par internet puisque le net a pour fonction la reproduction et la publication de textes ou d'opinions[39].

Par exemple, un journaliste publie un article avec des propos diffamants à l'encontre d'une personne sur son blog. Un blog a pour vocation de partager les informations contenues dans l'article à un grand nombre de personnes sur la toile. Son article pourrait être considéré comme un délit de diffamation commis par voie de presse.

3.4.3.2 La nécessité d'un écrit imprimé comme élément matériel

La nécessité d'un écrit imprimé a fait couler beaucoup d'encre car cet élément matériel du délit de presse a fait l'objet d'une interprétation différente par les juridictions et la doctrine.

D'une part, la Cour de cassation, dans un arrêt du 2 juin 2006[40], estime que les articles 25 et 150 de la Constitution ne s'appliquent pas aux délits sur internet étant donné qu'internet n'est pas un mode d'expression par écrit imprimé. La Cour de cassation et une partie de la doctrine justifient cette analyse comme suit: *"la version néerlandaise de la Constitution qui, adoptée en 1967, fait usage du terme "drukpers" (littéralement: presse imprimée), excluant ainsi la radio, la télévision et, peut-on supposer, internet des protections Constitutionnelles réservées à*

[38] Cass., 6 mars 2012, J.T., 2012, p. 505.
[39] DEBILIO, R., "Quand Internet s'invite dans la jurisprudence de la Cour de cassation: l'élément matériel du délit de presse se précise", R.D.T.I., 2013/1, n° 50, p. 83-92.
[40] Cass., (1re ch.), 02 juin 2006, Pas., 2006/5-6, p. 1302.

la presse"[41]*.* Les partisans de cette analyse prônent plutôt une interprétation restrictive du terme "écrit imprimé".

D'autre part, une autre partie de la doctrine et de la jurisprudence avance une interprétation téléologique de la presse. Selon eux, le constituant qui a adopté les articles 25 et 150 de la Constitution avait comme objectif de garantir la liberté d'expression et, à l'époque, la presse audiovisuelle et électronique n'existait pas encore. Il convient alors de tenir compte des avancées technologiques et de faire entrer internet dans le champ d'application de ces articles. Il s'agit ici d'une interprétation extensive. Ensuite, cet écrit doit être publié. Cette condition se remplit facilement sur les réseaux sociaux étant donné qu'Internet permet de voir les messages en permanence pour tout un chacun qui dispose d'un accès au réseau.

3.4.3.3 L'élément intellectuel

Quant à la condition de l'élément intellectuel, à savoir le partage d'une opinion illicite ou qui correspond à un abus de la liberté d'expression, elle ne pose aucune difficulté aux juridictions puisqu'il suffit que l'auteur manifeste une pensée illicite.

3.4.4 Arrêt de la cour d'appel de Mons du 14 mai 2008

Comme la théorie, selon laquelle il faudrait interpréter les articles 25 et 150 de la Constitution de manière téléologique, permet de sanctionner les délits de presse sur le net et que nous considérons qu'il est plus intéressant de voir comment les cours et tribunaux font pour ne pas suivre la jurisprudence de la Cour de cassation, nous approfondirons cet arrêt de la cour d'appel de Mons du 14 mai 2008[42].

Les faits sont les suivants: le prévenu était dans un train de la SNCB en première classe avec un abonnement de 2ème classe. Un incident a eu lieu entre lui et deux agents de la SNCB et il a été poursuivi pour cet incident. Le prévenu a alors publié sur le site "Navetteurs" deux articles sur un forum de discussion dans les-

[41] DONY, C., "La presse, une notion que le Constituant tarde à (re)définir ...", J.L.M.B., 2010/3, p. 137-142.
[42] Mons, 14 mai 2008, n° F-20080514-1, inédit (disponible sur, www.juridat.be; consulté le 27 octobre 2014).

quels des injures et des imputations calomnieuses figuraient à l'encontre de la SNCB et de ses agents.

La cour d'appel de Mons a en premier lieu, examiné et rappelé les conditions du délit de presse telles qu'elles sont établies par la Cour de cassation et elle a estimé que les textes que le prévenu a diffusés sur le site "Navetteurs.be" évoquent son opinion mais par des propos injurieux. De plus, l'écrit qui relate son histoire et ses propos a bénéficié d'une publicité réelle et effective puisque le forum de discussion est accessible à tous et à n'importe quelle heure.

Ensuite, la cour d'appel s'appuie sur une partie de la motivation de la Cour de cassation, à savoir que le forum de discussion: *"n'est certes pas un "imprimé" et sa reproduction ne dépend pas d'une activité d'imprimerie ou d'un moyen similaire à celle-ci (au sens strict et classique de ces termes)".* Et la cour d'appel y ajoute son propre raisonnement en disant que la reproduction de l'écrit sur Internet est illimitée puisque tous les surfeurs du net peuvent imprimer et diffuser les écrits litigieux. D'ailleurs, la cour d'appel a étendu l'application du délit de presse à Internet comme étant une évolution de la presse écrite comme repris-ci-dessous:

> *"Ce procédé de multiplication de l'écrit contenant son opinion, diffusé via le site internet "Navetteurs.be" est, à l'heure actuelle et compte tenu de l'évolution de la technologie, comparable et assimilable à celui de l'imprimerie et des moyens similaires à celle-ci visés par la Constitution".*

En conséquence, si le caractère calomnieux est retenu, le prévenu pourra être condamné pour délit de presse. Mais dans ce cas-ci, seule la cour d'assises est compétente pour juger le prévenu. La cour d'appel s'est donc déclarée incompétente et a confirmé le jugement en 1ère instance qui avait qualifié les faits reprochés de délit de presse et s'était également déclarée incompétente pour juger du litige.

3.5 LE RACISME ET LA XÉNOPHOBIE

3.5.1 Notions

Le dictionnaire Larousse définit le racisme comme étant:

> *"L'idéologie fondée sur la croyance qu'il existe une hiérarchie entre les groupes humains, les "races"; comportement inspiré par cette idéologie"*[43].

Mais il définit la xénophobie comme une "Hostilité systématique manifestée à l'égard des étrangers"[44].

Nous pouvons en déduire que le racisme crée des catégories de personnes qui doivent être traitées de façons différentes sur base d'une religion par exemple, alors que la xénophobie se caractérise par un traitement différent à l'égard des étrangers.

Ensuite, le combat contre le racisme et la xénophobie n'est pas récent. Mais il a pris de l'ampleur suite à l'apparition de la toile étant donné qu'Internet permet de toucher un nombre bien plus important de personnes que les messages écrits sur du papier et cela pour un coût dérisoire. De plus, contrôler tous les messages qui sont écrits sur les sites des internautes est tout simplement impossible.

Bien que la Constitution belge et la Convention de sauvegarde des Droits de l'Homme protègent le droit à la liberté d'expression, cette même Convention énonce dans son article 10, alinéa 2. (cité plus haut), la limite à la liberté d'expression. Il s'agit de la sauvegarde de la réputation des personnes et de la protection de la morale, c'est-à-dire les valeurs fondamentales d'une société démocratique, à savoir l'égalité dans ce cas-ci.

La Belgique, conformément à la Convention internationale sur l'élimination de toutes les formes de discrimination raciale du 21 décembre 1965, a pris une loi pour lutter contre le racisme et la xénophobie. Il s'agit de l'article 1 2° et 4° ainsi

[43] http://www.larousse.fr/dictionnaires/francais/racisme/65932
[44] http://www.larousse.fr/dictionnaires/francais/x%C3%A9nophobie/82881

que l'article 3 de la loi du 30 juillet 1981, tendant à réprimer certains actes inspirés par le racisme ou la xénophobie. Cette loi a été modifiée par la loi du 10 mai 2007 où ces articles sont devenus les articles 20, 21 et 22[45]. Chacun de ces articles présente un élément constitutif commun, l'article 444 du Code pénal cité plus haut. En d'autres mots, la première condition du racisme et de la xénophobie est le caractère public du message que nous avons déjà expliqué dans le passage sur la calomnie et la diffamation. (Chapitre 4, sous-section 3.2.2)

3.5.2 L'incitation à la haine raciale ou au racisme

Article 20*: "Est puni d'un emprisonnement d'un mois à un an et d'une amende de cinquante euros à mille euros, ou de l'une de ces peines seulement :*

- *Quiconque, dans l'une des circonstances indiquées à l'article 444 du Code pénal, incite à la discrimination à l'égard d'une personne, en raison de l'un des critères protégés, et ce, même en dehors des domaines visés à l'article 5;*

- *Quiconque, dans l'une des circonstances indiquées à l'article 444 du Code pénal, incite à la haine ou à la violence à l'égard d'une personne, en raison de l'un des critères protégés, et ce, même en dehors des domaines visés à l'article 5;*

- *Quiconque, dans l'une des circonstances indiquées à l'article 444 du Code pénal, incite à la discrimination ou à la ségrégation à l'égard d'un groupe, d'une communauté ou de leurs membres, en raison de l'un des critères protégés, et ce, même en dehors des domaines visés à l'article 5;*

- *Quiconque, dans l'une des circonstances indiquées à l'article 444 du Code pénal, incite à la haine ou à la violence à l'égard*

[45] Corr. Bruxelles (61 echambre), 27/11/2009, J.L.M.B., 2010/1, p. 10-17.

d'un groupe, d'une communauté ou de leurs membres, en raison de l'un des critères protégés, et ce, même en dehors des domaines visés à l'article 5".

Les critères protégés dans l'article 4 de la loi du 30 juillet 1981, tendant à réprimer certains actes inspirés par le racisme ou la xénophobie sont les suivants:

"Pour l'application de la présente loi, il y a lieu d'entendre par :

4° critères protégés: la nationalité, une prétendue race, la couleur de peau, l'ascendance ou l'origine nationale ou ethnique".

L'auteur qui incite à la discrimination ou à la violence à l'égard d'une personne ou d'un groupe en raison de la nationalité, une prétendue race, la couleur de peau, l'ascendance ou l'origine nationale ou ethnique pourra être condamné.

3.5.3 La diffusion du racisme et de la xénophobie sur internet

Article 21: *"Quiconque, dans l'une des circonstances indiquées à l'article 444 du Code pénal, diffuse des idées fondées sur la supériorité ou la haine raciale, est puni d'un emprisonnement d'un mois à un an et d'une amende de cinquante euros à mille euros, ou de l'une de ces peines seulement".*

Pour être condamné, l'auteur des propos doit avoir diffusé des idées sur la supériorité (racisme) ou de la haine raciale (xénophobie): c'est l'élément matériel du délit. Quant à l'élément moral, il s'agit d'un dol général. Pour rappel, le tribunal civil de Bruxelles a admis que la diffusion sur internet est une communication publique si l'accès est ouvert à tous. (Chapitre 4, sous-section 3.2.3)

3.5.4 Les associations qui prônent le racisme et la xénophobie

De la même manière que sont sanctionnés les auteurs de messages racistes ou xénophobes, les membres d'une association prônant le racisme ou la xénophobie peuvent aussi être condamnés par la loi sur le racisme et la xénophobie:

> **Article 22***: "Est puni d'un emprisonnement d'un mois à un an et d'une amende de cinquante euros à mille euros, ou de l'une de ces peines seulement, quiconque fait partie d'un groupement ou d'une association qui, de manière manifeste et répétée, prône la discrimination ou la ségrégation fondée sur l'un des critères protégés dans les circonstances indiquées à l'article 444 du Code pénal, ou lui prête son concours".*

L'élément matériel est la participation à un groupe qui prône le racisme ou la xénophobie, c'est-à-dire des idées où il existe des hiérarchies entre les individus. Ensuite, il faut que les membres prônent le racisme ou la xénophobie de manière répétée et manifeste (dol spécial).

Dans le cadre d'internet, cette condition peut être remplie dès lors que les messages restent visibles sur le site internet. L'exemple typique tiré de la doctrine où l'on peut considérer qu'il s'agit d'un groupement sur internet sont "*les forums de discussion, où circulent nombre de messages racistes ou xénophobes, constituent de telles associations prônant le racisme*"[46].

3.5.5 Jurisprudence

Le tribunal correctionnel de Bruxelles a rendu un jugement le 27 novembre 2009.[47] Le juge a dû se prononcer sur une incitation à la discrimination sur le site du Front National Belge.

La prévenue B. a été éditeur et auteur de la revue "le *Bastion"* dans laquelle figuraient des incitations à la discrimination. De plus, la prévenue était au courant de l'existence du site hébergé en Belgique puis en Océanie où son périodique était publié. Elle n'a jamais exigé que ses publications soient retirées du site alors qu'elle en avait la possibilité.

La prévenue a demandé au tribunal correctionnel de poser une question préjudicielle à la cour Constitutionnelle pour savoir si l'article premier, 2° et 4° de la loi du

[46] POULLET, Y., La lutte contre le racisme et la xénophobie sur l'internet, J.T., 2006/23, n° 6229, p. 401-412.
[47] Corr. Bruxelles (61 ^{e}chambre), 27/11/2009, *J.L.M.B.*, 2010/1, p. 10-17.

30 juillet 1981 n'était pas contraire à l'article 10 de la Convention européenne des droits de l'homme. Mais le tribunal estime que *" L'entrave que constitue cet article à la liberté d'expression est, en effet, nécessaire dans une société qui se veut démocratique et dans laquelle aucun discours appelant à la violence et à la discrimination, de quel type qu'elles soient, n'est pas admissible".*

Au vu des textes publiés sur le site du FNB, le tribunal a jugé que ces textes incitaient à la discrimination. De plus, la prévenue B. en a fait la publicité sur un site internet, ce qui est une des circonstances visées par l'article 444 du Code pénal. Sur base de ces éléments, le tribunal a considéré que les charges étaient établies dans le chef de la prévenue.

3.5.6 La charge de la preuve

La loi du 30 juillet 1981 tendant à réprimer certains actes inspirés par le racisme ou la xénophobie prévoit des dispositions spécifiques en matière de charge de la preuve:

> **Article 30**: *"§ 1er. Lorsque qu'une personne qui s'estime victime d'une discrimination, le Centre ou l'un des groupements d'intérêts invoque devant la juridiction compétente des faits qui permettent de présumer l'existence d'une discrimination fondée sur l'un des critères protégés, il incombe au défendeur de prouver qu'il n'y a pas eu de discrimination".*

Le Centre désigne le Centre pour l'égalité des chances et la lutte contre le racisme. En principe, il appartient à la victime de prouver les faits qu'elle invoque mais, dans le cadre de la lutte contre le racisme et la xénophobie, le législateur a voulu faciliter le travail de la victime en instaurant un partage de la preuve en matière de racisme ou de xénophobie.

Cela signifie que la victime ou le Centre devra apporter des éléments assez convaincants et troublants[48] pour faire naître une présomption réfragable de discrimi-

[48] BOUBKIRA, I., "La charge de la preuve en matière de discrimination", J.D.J., 2011/8, n° 308, p. 20-28.

nation sur base de l'un des critères protégés. Il appartiendra au prévenu de prouver le caractère non-discriminatoire des faits.

3.5.6.1 Une discrimination fondée sur l'un des critères protégés

Lorsque la discrimination est basée sur la nationalité, une prétendue race, la couleur de peau, l'ascendance ou l'origine nationale ou ethnique, la victime peut se prévaloir du partage de la charge de la preuve. Dans les autres cas, il appartient à la victime de prouver les faits à caractère raciste ou xénophobe.

3.5.6.2 Les faits que doit prouver la victime pour une discrimination directe

> **Article 30**: *"§ 2. Par faits qui permettent de présumer l'existence d'une discrimination directe fondée sur un critère protégé, sont compris, entre autres, mais pas exclusivement:*
>
> - *"1° Les éléments qui révèlent une certaine récurrence de traitement défavorable à l'égard de personnes partageant un critère protégé; entre autres, différents signalements isolés faits auprès du Centre ou l'un des groupements d'intérêts; ou*
> - *"2° les éléments qui révèlent que la situation de la victime du traitement plus défavorable est comparable avec la situation de la personne de référence".*

Tout d'abord, l'expression "*sont compris entre autres, mais pas exclusivement*" signifie que la loi sur le racisme et la xénophobie donne d'autres modes de preuve mais que les modes de preuve du droit civil ne sont pas exclus. Ainsi, l'aveu, le témoignage ou encore l'écrit peuvent être utilisés pour prouver une discrimination directe ou indirecte.

Ensuite, les éléments qui révèlent une récurrence se prouvent par un test de récurrence. Ce test se base sur les signalements des victimes au centre pour vérifier l'existence d'un comportement répétitif et défavorable envers les personnes qui n'ont que l'un des critères protégés comme point commun. Si un tel comportement

est observé, par exemple dans une entreprise dans sa politique d'embauche, il y aura une présomption de discrimination.

Pour finir, le traitement défavorable se prouve par un test de comparabilité. La doctrine en donne une définition: ce test "*consiste à comparer la situation de la victime potentielle de discrimination avec celle d'une personne dite de référence qui se distingue uniquement par l'absence du critère protégé dont la victime est porteuse. Dès lors en cas de traitement diffèrent, on présumera que c'est le critère protégé qui en est à l'origine*"[49].

Par exemple, le tribunal correctionnel de Bruxelles a rendu un jugement le 31 mars 2004[50]. Dans les faits, le gérant d'une agence immobilière a refusé de fournir ses services à un client sur base de son origine congolaise. La victime a organisé un test de situation avec le Centre. Un ami "belgo-belge" a demandé les mêmes renseignements que le demandeur et il n'a eu aucun problème pour obtenir les services du gérant. Sur base de ce test et des aveux du gérant, le tribunal correctionnel condamna le défendeur.

3.5.6.3 Les faits que doit prouver la victime pour une discrimination indirecte

> **Article 30**: *"§ 3. Par faits qui permettent de présumer l'existence d'une discrimination indirecte fondée sur un critère protégé, sont compris, entre autres, mais pas exclusivement:*
>
> - *1° Des statistiques générales concernant la situation du groupe dont la victime de la discrimination fait partie ou des faits de connaissance générale; ou*
> - *2° l'utilisation d'un critère de distinction intrinsèquement suspect; ou*
> - *3° du matériel statistique élémentaire qui révèle un traitement défavorable".*

[49] BOUBKIRA, I., "La charge de la preuve en matière de discrimination ", J.D.J., 2011/8, n° 308, p. 20-28.

[50] Corr. Bruxelles (55ème ch.), 31 mars 2004,

Nous citons ce paragraphe dans un but informatif car il parle du test de statistique. Ce test consiste à créer deux groupes. Un groupe de départ de référence et un groupe d'arrivée dans lesquels il faudra distinguer les personnes présentant l'un des critères protégés. Puis, il faut calculer combien de personnes présentent un critère protégé dans le groupe de référence et combien de ces personnes se retrouvent dans le groupe d'arrivée. Si l'écart entre les chiffres est trop élevé, il y a présomption d'une discrimination indirecte.

Mais ce test est difficile à réaliser dans la réalité. En effet, il exige que le nombre de personnes y participant soit assez important. De plus, l'écart peut aussi être dû au hasard et les chiffres peuvent également être faux.

3.6 JE SUIS VICTIME, QUE FAIRE?

3.6.1 Procédure pénale

Il y a peu de choses à dire sur la procédure pénale par rapport aux délits commis sur internet puisque la procédure est la même que pour les délits normaux, à une exception près lors de la phase préparatoire: les victimes ne peuvent pas toujours être sûres que les contenus qu'elles consultent sur le net sont illicites ou ne sont pas protégés par la liberté d'expression.

La Federal Computer Crime Unit a mis en ligne une plateforme permettant aux internautes de signaler les contenus illicites que les particuliers repèrent sur la toile. Cette plateforme se nomme "eCops". Tout d'abord, l'internaute remplit un questionnaire, puis la Federal Computer Crime Unit examine le site. Si elle estime que le contenu est illicite, l'information remonte au parquet qui se charge de la suite. Le reste se déroule comme une procédure pénale normale.

Dernière chose, il est aussi possible de contacter le fournisseur d'accès pour obtenir des informations comme l'adresse IP d'une personne soupçonnée d'avoir posté un contenu illicite sur internet. Mais il faut faire vite car les fournisseurs d'accès sont tenus de conserver ces informations pendant un an seulement.

3.6.2 Au niveau de la preuve

3.6.2.1 Difficulté de rapporter la preuve

Comme nous l'avons vu, il incombe à la victime de démontrer les faits, sauf exception pour le racisme et la xénophobie où il y a un partage de preuve. Pour démontrer des faits sur internet, il faut savoir que le juge considérera comme insuffisantes toutes les pièces fournies par la victime. Il existe donc un doute sur l'authenticité de la preuve, car il est possible de modifier sur l'ordinateur la pièce fournie au juge. Cette pièce sera considérée comme insuffisante pour établir la culpabilité du prévenu.

En conséquence, il est extrêmement difficile de rapporter une preuve d'internet puisque tout ce qui est présent sur un site web peut être modifié par l'internaute. Par exemple, il est possible de modifier les mots d'un site web et de les remplacer par des déclarations illicites, puis faire une capture d'écran en guise de preuve pour le juge. Cette volatilité des contenus est une caractéristique propre à internet qui rend la poursuite des infractions difficile puisque toutes les pièces que la victime produira devant le juge ne seront que des présomptions de l'homme. En conséquence, le prévenu pourra facilement mettre en doute l'authenticité des preuves.

3.6.2.2 Solution: le constat d'huissier

En France, l'huissier a le pouvoir de dresser des constats afin de constituer une preuve des contenus sur le net. Cependant, un constat d'huissier sera considéré ici comme une présomption de l'homme et ne pourra être produit en justice que si la preuve par témoin est admissible. De plus, un tel constat doit contenir un certain nombre de mentions pour être valable.

Tout d'abord, sur le contenu du constat, l'huissier ne pourra que constater des faits purement matériels et il ne peut en aucun cas fournir un avis. Le but de cette mention est de garantir une neutralité dans le constat. L'objectivité d'un constat d'huissier sera souvent privilégiée par rapport à la preuve rapportée par l'une des parties.

Ensuite, l'huissier doit indiquer les mentions légales prévues à l'article 43 du Code judiciaire, notamment la date et le lieu, les coordonnés de l'huissier et celles du requérant. Mais, sur internet, d'autres éléments techniques sont obligatoires pour que le constat soit valable. Ces éléments techniques permettent au magistrat d'apprécier la valeur du constat au niveau probatoire.

Du point de vue du matériel informatique utilisé, l'huissier doit indiquer et veiller à mettre à jour:

- le système d'exploitation (Windows, Linux,…) ainsi que sa version,
- le navigateur internet (Internet Explorer, Firefox, Opera, Google Chrome, …),
- les plug-ins et leurs versions.

Ensuite, au niveau de la connexion internet, l'huissier devra indiquer l'adresse IP et le serveur proxy car celui-ci joue un rôle de mémoire tampon dans un but de rapidité dans le chargement des pages web. Le serveur proxy stocke une copie de la page web qui peut être modifiée et qui est la première page à laquelle l'huissier va se connecter, mais cette page ne sera pas la page la plus récente ou cette page ne sera pas la même.

Quant à l'adresse IP, elle sert à vérifier que l'huissier s'est effectivement rendu sur la page litigieuse à un moment précis. En France, l'absence d'adresse IP exclut souvent le constat d'huissier des débats.

Pour finir, Le navigateur internet que l'huissier utilise doit en premier lieu être vidé de ses fichiers temporaires. Ces fichiers sont aussi des copies de pages web falsifiables qui fonctionnent un peu comme le serveur proxy. Cette obligation empêche l'utilisateur de modifier les fichiers temporaires puis que celui-ci demande un constat à l'huissier

CHAPITRE 5: LA RESPONSABILITÉ CIVILE

1 INTRODUCTION

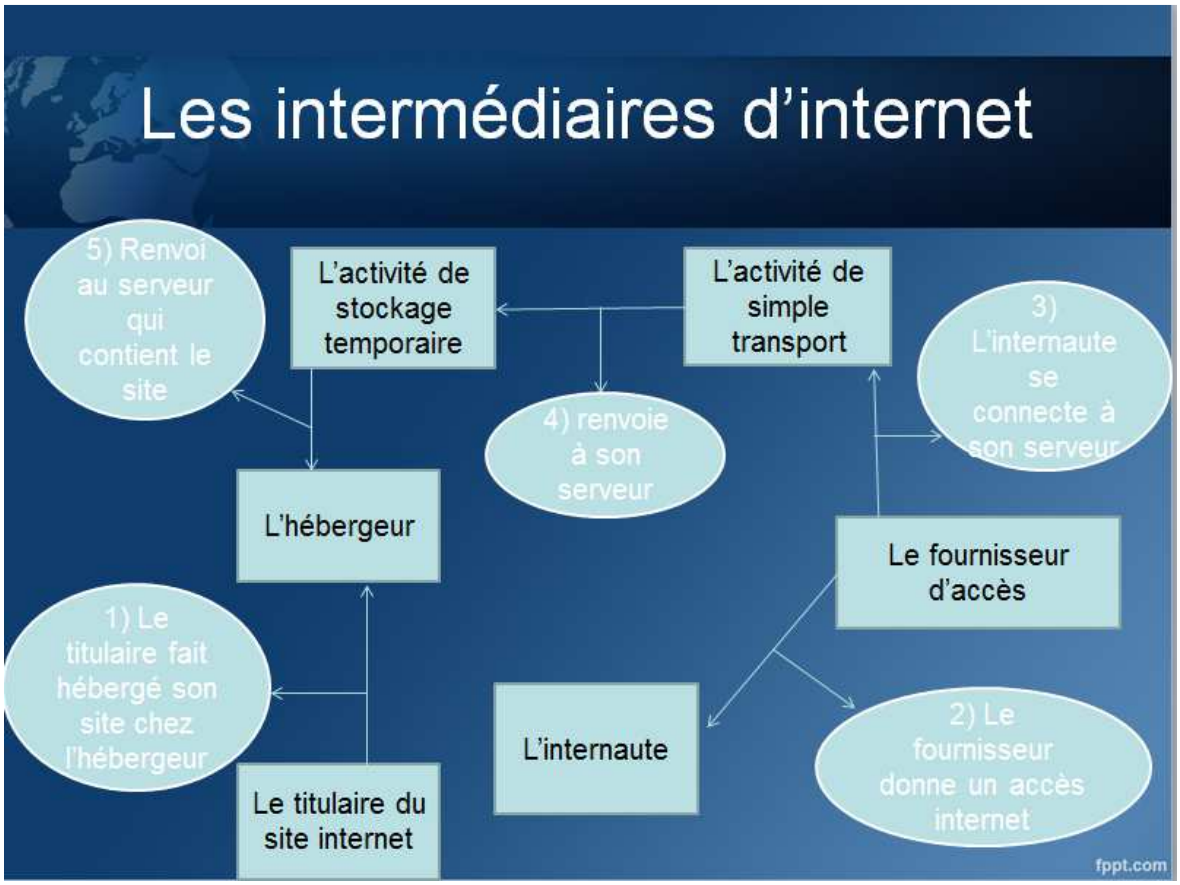
La responsabilité des prestataires mérite un chapitre à elle seule puisqu'elle est le premier moyen pour lutter contre les contenus illicites. Pourquoi? Parce que les prestataires fournissent un accès aux contenus illicites et parce que les prestataires peuvent bloquer l'accès à ces contenus.

Vu que le principal problème en matière de cybercriminalité réside dans la difficulté de découvrir le coupable, soit parce qu'il est à l'étranger, soit parce que la police ne parvient pas à l'identifier ou même, si elle y arrive, parce que le coupable est insolvable, le droit belge a offert aux victimes une possibilité d'engager la responsabilité de tous les acteurs du net connus de tous et surtout bien plus solvables.

Bien sûr, la responsabilité des prestataires peut être engagée au pénal. Le prestataire peut être condamné aux peines prévues dans le Code pénal, ainsi que je l'ai développé plus haut au chapitre 4, et, dans cette hypothèse, la victime se sera constituée partie civile devant la juridiction pénale afin d'obtenir des dommages et intérêts et/ou de demander au juge que les prestataires prennent des mesures pour faire cesser la diffusion du contenu litigieux.

Toutefois, s'il n'y a pas de procédure pénale engagée, la responsabilité civile des prestataires peut être mise en cause devant la juridiction civile. La victime réclamera également des dommages et intérêts et/ou demandera au juge que les prestataires retirent le contenu litigieux. Néanmoins, il n'est pas facile d'identifier le rôle de chaque prestataire sur le net. Nous vous proposons donc le schéma ci-dessous et repris en annexe[51].

[51] Voir annexe n° 7



Celui-ci montre que le titulaire du site va payer un hébergeur pour publier son site sur la toile et le rendre accessible à tous. Ensuite, l'internaute qui veut consulter ce site va se connecter à un serveur internet grâce à son fournisseur d'accès. Ce serveur est souvent celui d'un prestataire effectuant une activité de simple transport: il va rediriger l'internaute vers le serveur de l'hébergeur ou celui d'un prestataire qui effectue une activité de simple stockage et qui a gardé une copie du site que l'internaute veut consulter.

2 LE PRINCIPE GÉNÉRAL DE RESPONSABILITÉ CIVILE DES INTERMÉDIAIRES

2.1 L'ARTICLE 1382 DU CODE CIVIL

La responsabilité civile des prestataires d'internet se déduit de l'article 1382 du Code civil:

> **Article 1382**: *"Tout fait quelconque de l'homme, qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé, à le réparer".*

Cet article ne s'applique que si le prestataire a commis une faute en lien causal avec le dommage subi par la victime. Dans le contexte d'internet, la faute commise est d'insérer et/ou de laisser un contenu préjudiciable sur un réseau électronique. Néanmoins, la jurisprudence n'est pas des plus claires dans cette matière.

D'une part, les décisions varient d'un pays à l'autre puisque les lois sont différentes d'un pays à l'autre et même d'un magistrat à l'autre au sein du même pays. D'autre part, il est parfois difficile de savoir si une faute est commise sur internet. Par exemple, le tribunal civil d'Anvers[52] s'est prononcé sur la faute. Dans les faits, le demandeur avait trouvé des propos diffamants le concernant sur le forum du défendeur et avait demandé le retrait de ce contenu. Mais le tribunal a estimé qu'il n'y avait pas de faute vu que le contenu avait été retiré et que le demandeur consultait en fait une page stockée en mémoire cache illisible pour les autres.

Il convient aussi d'établir le lien entre l'article 1382 du Code civil et les conditions de restriction de la liberté d'expression prévues à l'article 10, alinéa 2, de la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales, à savoir que la restriction doit être prévue par la loi. En effet, l'article 1382 du Code civil est l'exemple type d'une norme vague dont l'application à Internet n'est pas prévue par la loi. Dès lors, il appartient à la jurisprudence de définir clairement l'application de l'article 1382 du Code civil aux atteintes sur la toile comme l'a fait le tribunal civil d'Anvers.

[52] Civ. Anvers (5ème ch. B), 3 décembre 2009, 09/1322/A, A. & M., 2010/5-6, p. 560-562.

2.2 L'APPLICATION DE L'ARTICLE 1382 DU CODE CIVIL À L'AUTEUR OU LE WEBMASTER DU CONTENU JUGÉ ILLICITE

2.2.1 L'auteur du contenu litigieux

L'auteur des contenus litigieux est rarement le plus solvable ou le plus facile à appréhender. Une solution intéressante a été mise en place grâce aux fournisseurs d'accès qui connaissent le nom du client et l'adresse IP associée à ce client et conservent pendant un an au minimum ces informations qu'ils sont tenus de divulguer aux autorités, comme le parquet par exemple, lorsqu'elles en font la demande.

Cependant, en matière civile, il sera difficile d'obtenir la réparation du dommage causé via le principe de l'article 1382 du Code civil par l'obtention d'une indemnité (pécuniaire) si le coupable est insolvable. Cette difficulté explique pourquoi le droit a reconnu la responsabilité des prestataires de service afin de ne pas laisser les victimes sans une indemnité.

2.2.2 Le webmaster d'un site présentant un contenu litigieux

Quant au titulaire du site ou "webmaster", il ne bénéficie pas d'une exonération de responsabilité puisqu'il ne fait pas partie des prestataires de la loi du 15 décembre 2013. Il est même considéré par la directive sur le commerce électronique comme un destinataire de service et non comme un prestataire.

D'ailleurs, l'auteur du contenu illicite peut également être le titulaire du site ou non. S'il ne l'est pas, il est alors un éditeur et agit en qualité de "webmaster". Lorsque la responsabilité d'un "webmaster" est mise en cause, le tribunal devra examiner le ou les rôles qu'a remplis le titulaire du site. Ainsi, le tribunal correctionnel de Bruxelles a déclaré le 23 juin 2009[53] qu'un titulaire de site qui remplit une fonction purement technique ne peut être tenu pour responsable du contenu dans le contexte de la responsabilité en cascade décrit plus loin. Alors que si le titulaire du site assume l'édition du contenu illicite, la doctrine considère que *"le titulaire d'un*

[53] Corr. Bruxelles (54ème ch.), 23 juin 2009, J.L.M.B., 2010/3, p. 123-127.

site Web est naturellement responsable du contenu qu'il met en ligne, à l'égard duquel il assume une fonction d'éditeur"[54].

Il faut aussi souligner que le titulaire du site peut se voir contraint de surveiller son site puisqu'il n'est pas protégé par la loi du 15 décembre 2013, à moins qu'il ne soit simple hébergeur, mais ce cas est rare, par exemple, un site de petites annonces.

2.3 LES PRESTATAIRES POUVANT BÉNÉFICIER D'UNE EXONÉRATION

Les dispositions relatives à certains prestataires sont prévues dans la loi du 15 décembre 2013[55] qui transpose la directive n° 2000/31 du Parlement européen et du Conseil du 8 juin 2000 sur le commerce électronique[56]. La loi du 15 décembre 2013 abroge la loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information mais elle conserve à l'identique les dispositions relatives aux exonérations des intermédiaires.

Il convient surtout de noter que la loi du 15 décembre 2013 donne des conditions d'exonération de responsabilité civile et pénale plutôt que définir les responsabilités civiles. En conséquence, l'article 1382 du Code civil est en principe d'application pour engager la responsabilité d'un prestataire d'internet sauf si celui-ci est reconnu comme intermédiaire au sens de la loi du 15 décembre 2013 et bénéficie de par cette loi d'une exonération.

2.3.1 Champ d'application de la loi du 15 décembre 2013

Pour être reconnu comme un prestataire au sens de la loi du 15 décembre 2013, le prestataire doit être: "*toute personne physique ou morale qui fournit un service*

[54] WÉRY, E., "Internet hors la loi? Description et introduction à la responsabilité des acteurs du réseau", J.T., 1997, p. 419.
[55] L. du 15 décembre 2013 portant insertion du Livre XII, " Droit de l'économie électronique " dans le Code de droit économique, portant insertion des définitions propres au Livre XII et des dispositions d'application de la loi propres au Livre XII, dans les Livres I et XV du Code de droit économique. M.B., le 14 janvier 2014, p. 1524.
[56] Directive (CE) n° 2000/31 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), J.O.C.E., n° L 178 du 17 juillet 2000, p. 1.

de la société de l'information", c'est-à-dire: "*tout service presté normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire du service*". Nous pouvons déduire de cette définition que les prestataires visés par la loi du 15 décembre 2013 doivent rendre un service à distance, à titre onéreux et fondé sur une demande d'un destinataire de service.

Toutefois, cette définition étant plutôt floue, la Cour de cassation a trouvé une définition contenant deux conditions pour considérer que le prestataire soit exonéré: "*ces dispositions ne prévoient l'exclusion de la responsabilité que pour chaque prestataire de services qui agit en tant qu'intermédiaire au sens de cette loi du 11 mars 2003, dans la mesure où son activité revêt un caractère purement technique, automatique et passif, ce qui implique que l'intermédiaire ne connaît pas et n'exerce pas de contrôle sur l'information qui est transmise ou stockée*"[57].

En résumé, un prestataire au sens de la loi du 15 décembre 2013 est tout prestataire qui ignore et ne contrôle pas l'information. Si l'une des conditions dégagées par la Cour de cassation n'est pas remplie, la responsabilité de l'intermédiaire pourra être engagée sur base de l'article 1382 du Code civil. Voici les activités exonérées par la loi du 15 décembre 2013.

2.3.2 Les prestataires remplissant une activité de simple transport

Le simple transport concerne les fournisseurs de l'infrastructure qui transmettent les informations d'un serveur à l'autre et les fournisseurs d'accès qui donnent un accès à internet aux particuliers, c'est-à-dire la mise à disposition d'une connexion au réseau. Les informations sont copiées temporairement sur les serveurs des intermédiaires afin de passer d'un serveur à l'autre[58].

De plus, il existe des techniques informatiques qui permettent d'empêcher le fournisseur d'accès de voir les informations, d'où la nécessité de prévoir une exonération dans la loi du 15 décembre 2013:

[57] Cass., (2e ch.), 3 février 2004, R.D.T.I., 2004/2, p. 51.
[58] Voir annexe n° 8

Article XII.17: *"le prestataire de services n'est pas responsable des informations transmises, s'il est satisfait à chacune des conditions suivantes :*

1° il n'est pas à l'origine de la transmission;

2° il ne sélectionne pas le destinataire de la transmission;

3° il ne sélectionne, ni ne modifie, les informations faisant l'objet de la transmission".

Ces conditions sont cumulatives, le prestataire ne doit pas être l'auteur des informations qui sont transmises par son serveur, sinon il prend un rôle actif et s'implique dans la diffusion de l'information. Or, l'exonération ne couvre que le transfert passif de l'information.

Ensuite, le prestataire ne choisit pas le destinataire de l'information, il ne fait que faire passer l'information sur son serveur et remet l'information au destinataire choisi par son client. Enfin, le prestataire ne peut pas modifier les informations, sinon il aurait encore un rôle actif dans la diffusion du contenu illicite.

En revanche, même si le fournisseur d'accès ou d'infrastructure prend connaissance d'un contenu illicite, il pourra quand même être exonéré puisque la connaissance du transporteur de la présence d'un contenu litigieux ne fait pas partie des conditions d'exonération de la responsabilité.

Cette condition a été retirée par la directive sur le commerce électronique sur base des considérants n° 43 et 44 puisque le simple transport "*suppose que le prestataire n'est impliqué en aucune façon dans l'information transmise et deuxièmement, l'exonération ne bénéficie pas au prestataire qui collabore délibérément avec l'un des destinataires de son service. La logique sous-jacente est ici d'éviter toute forme de censure de leur part. Les opérateurs de réseaux et fournisseurs d'accès se doivent d'être neutres à l'égard des contenus diffusés et de n'interférer en aucune manière*"[59].

[59] V. KAISER, "La protection des mineurs sur Internet: la problématique de la pédopornographie et des contenus jugés préjudiciables", 2010.

2.3.3 Les prestataires remplissant une activité de stockage temporaire

Lors de cette activité également connue sous le nom de "caching", le prestataire stocke temporairement et automatiquement l'information en vue de rendre plus rapide sa transmission aux autres destinataires de service qui enverront cette même information.

Cette activité se distingue du simple transport par l'objectif du stockage temporaire qui est ici de décongestionner le réseau. La loi du 15 décembre 2013 exonère les prestataires exerçant une activité de stockage temporaire.

> **Article XII.18**: "*Le prestataire n'est pas responsable au titre du stockage automatique, intermédiaire et temporaire de cette information fait dans le seul but de rendre plus efficace la transmission ultérieure de l'information à la demande d'autres destinataires du service, pour autant que chacune des conditions suivantes soit remplie :*
>
> *1° le prestataire ne modifie pas l'information;*
>
> *2° le prestataire se conforme aux conditions d'accès à l'information;*
>
> *3° le prestataire se conforme aux règles concernant la mise à jour de l'information, indiquées d'une manière largement reconnue et utilisée par les entreprises;*
>
> *4° le prestataire n'entrave pas l'utilisation licite de la technologie, largement reconnue et utilisée par l'industrie, dans le but d'obtenir des données sur l'utilisation de l'information;*
>
> *5° le prestataire agit promptement pour retirer l'information qu'il a stockée ou pour rendre l'accès à celle-ci impossible dès qu'il a effectivement connaissance du fait que l'information à l'origine de la transmission a été retirée du réseau ou du fait que l'accès à l'information a été rendu impossible, ou du fait qu'une autorité administrative ou judiciaire a ordonné de retirer l'information ou de rendre l'accès à cette dernière impossible et pour au-*

tant qu'il agisse conformément à la procédure prévue à l'article XII.19, § 3".

Notons encore une fois que les conditions d'exonération de responsabilité sont cumulatives. Les autres conditions sont assez claires pour ne pas nécessiter d'explications supplémentaires, sauf en ce qui concerne la dernière condition. En effet, le prestataire n'est tenu de retirer ou de bloquer les contenus stockés que s'il a une connaissance effective que ce contenu a été retiré d'internet, bloqué ou qu'une autorité a donné l'ordre de retirer ou de bloquer le contenu litigieux. Nous reviendrons sur la connaissance effective lorsque nous aborderons la responsabilité de l'hébergeur. Dans le cadre de la cinquième condition, le prestataire doit en plus respecter une procédure:

"§ 3. Lorsque le prestataire a une connaissance effective d'une activité ou d'une information illicite, il les communique sur le champ au procureur du Roi qui prend les mesures utiles conformément à l'article 39bis du Code d'instruction criminelle.

"Aussi longtemps que le procureur du Roi n'a pris aucune décision concernant le copiage, l'inaccessibilité et le retrait des documents stockés dans un système informatique, le prestataire peut uniquement prendre des mesures visant à empêcher l'accès aux informations".

Lorsque les prestataires, remplissant une activité de stockage temporaire ou l'hébergement, ont connaissance d'un contenu illicite, ils ont un devoir d'intervention. Ils doivent informer le procureur du roi de la présence d'un contenu litigieux et bloquer l'accès au contenu, tant que le procureur du roi n'a pas pris de décision. Cette procédure pose problème car les prestataires sont les premiers juges du contenu illicite. Or, il appartient au juge de statuer sur ce qui est licite ou pas.

Si les prestataires retirent le contenu litigieux ou en bloquent l'accès et que ce contenu était licite, c'est une atteinte à la liberté d'expression. Si ce contenu était illicite et qu'il n'a pas été bloqué, les prestataires peuvent alors être déclarés

responsables. Cette position du prestataire lui est inconfortable étant donné qu'il n'est pas en mesure d'apprécier si un contenu est licite ou non.

2.3.4 L'hébergeur

La loi du 15 décembre 2013 donne une définition précise de ce qu'est l'activité d'hébergeur: il s'agit de la "*fourniture d'un service de la société de l'information consistant à stocker des informations fournies par un destinataire du service*". Un travail de réflexion a été accompli par la doctrine afin de déterminer si un lien de propriété devait exister entre le prestataire et le serveur sur lequel est stocké le contenu litigieux.

Cependant, certains prestataires qui préfèrent louer un serveur pour réaliser une activité hébergement ne seraient pas visés par l'exonération. De plus, la définition donnée par la loi du 15 décembre2013 est écrite avec des termes larges. En définitive, cette condition de lien de propriété n'a pas été retenue. La doctrine a ensuite proposé une définition plus précise: "*l'activité d'hébergement consiste donc à stocker des informations fournies par des tiers et à leur demande sur un espace appartenant au prestataire ou non*[60]". En bref, les hébergeurs répondant à cette définition peuvent se voir exonérés de responsabilité civile et pénale par la loi du 15 décembre 2013 dans deux cas:

> **Article XII. 19 §1er** "*le prestataire n'est pas responsable des informations stockées à la demande d'un destinataire du service à condition:*
>
> *1° qu'il n'ait pas une connaissance effective de l'activité ou de l'information illicite, ou, en ce qui concerne une action civile en réparation, qu'il n'ait pas connaissance de faits ou de circonstances laissant apparaître le caractère illicite de l'activité ou de l'information; ou*
>
> *2° qu'il agisse promptement, dès le moment où il a de telles connaissances, pour retirer les informations ou rendre l'accès à celles-ci impos-*

[60] DE PATOUL, F., VEREECKEN, I., "La responsabilité des intermédiaires de l'internet: première application de la loi belge", R.D.T.I., 2004/2, p. 54.

sible et pour autant qu'il agisse conformément à la procédure prévue au paragraphe 3".

2.3.4.1 Absence de connaissance effective

Les hébergeurs qui prouvent qu'ils n'avaient pas connaissance de la présence de contenus illicites sur le site qu'ils hébergent sont exonérés.

Il existe deux niveaux de connaissance:

- La connaissance circonstanciée qui est le minimum pour intenter une action en dommages et intérêts ou pour demander le retrait du contenu litigieux. La doctrine considère que ce degré de connaissance est atteint s'il résulte "*de faits ou de circonstances selon lesquels l'activité ou l'information illicite est apparente*"[61].
- La connaissance effective nécessaire en matière pénale. Ce degré de connaissance est souvent atteint lors de l'envoi d'une notification. Cependant, la loi du 15 décembre 2013 ne précise pas les informations à notifier pour que le juge considère que le prestataire ait la connaissance effective.

À titre d'illustration, le tribunal de commerce de Bruxelles a condamné, dans un jugement du 2 novembre 1999[62], la société Belgacom Skynet pour avoir hébergé des sites qui renvoyaient à des contenus illicites. La société Belgacom Skynet ne les avaient pas supprimés alors que la partie demanderesse avait mis en demeure la société Belgacom Skynet de les retirer. "*Le tribunal considère que la société Belgacom Skynet est responsable lorsqu'elle ne supprime pas les liens litigieux alors qu'elle a été mise au courant d'activités suspectes*"[63].

2.3.4.2 Agir promptement pour retirer les contenus illicites

La deuxième possibilité consiste à agir promptement pour retirer les contenus illicites ou en bloquer l'accès dès qu'ils ont eu connaissance de leur présence, sous

[61] STROWEL, A., IDE, N. et VERHOESTRAETE, F., "La directive du 8 juin 2000 sur le commerce électronique: un cadre juridique pour l'Internet", J.T., 2001/7, n° 6000, p. 133-145.
[62] Comm. Bruxelles, 2 novembre 1999, A. & M., 2000, p. 474.
[63] VERBIEST T., WERY E., La Responsabilité des fournisseurs de services internet: dernier développements jurisprudentiels, J.T., 2001, p. 165-173.

réserve de la procédure du paragraphe 3 que nous avons abordée précédemment. (Chapitre 5, sous-section 3.3).

Pour finir, une grande incertitude et une insécurité continuent de planer sur les hébergeurs au vu du manque de précision des termes employés dans la loi du 15 décembre 2013.

2.3.5 L'absence d'obligation de surveillance pour les prestataires visés par la loi du 15 décembre 2013

> **Article XII. 20***: "§ 1er. Pour la fourniture des services visés aux articles XII.17, XII.18 et XII.19, les prestataires n'ont aucune obligation générale de surveiller les informations qu'ils transmettent ou stockent, ni aucune obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites".*

En résumé, les prestataires, exerçant une activité visée par la loi du 15 décembre 2013, ne peuvent recevoir de l'État l'obligation de surveiller de manière générale les informations de tous les clients qu'ils transmettent ou qu'ils stockent. L'objectif du législateur était de couvrir la responsabilité en cas d'utilisation de logiciels de filtrage ou de blocage par mot-clé. Cette couverture trouve son origine dans l'automatisation de ces logiciels et personne ne surveille leur exécution.

De plus, une telle surveillance serait un poids trop lourd à porter pour les prestataires d'internet. Toutefois, ceux-ci sont libres de surveiller et de rechercher les contenus illicites s'ils le souhaitent. Par contre, une surveillance particulière peut être imposée, à condition qu'elle soit prévue par la loi, ce qui est le cas dans la loi du 15 décembre 2013:

> **Article XII. 20 §1, alinéa 2**:*"Le principe énoncé à l'alinéa 1er ne vaut que pour les obligations à caractère général. Il n'empêche pas les autorités judiciaires compétentes d'imposer une obligation temporaire de surveillance dans un cas spécifique, lorsque cette possibilité est prévue par une loi".*

2.4 CAS PARTICULIER DE LA RESPONSABILITÉ EN CASCADE EN MATIÈRE DE DÉLIT DE PRESSE

Cette responsabilité particulière se déduit de l'article 25 de la Constitution qu'il me paraît utile de rappeler ici:

> **Article 25***: "La presse est libre; la censure ne pourra jamais être établie; il ne peut être exigé de cautionnement des écrivains, éditeurs ou imprimeurs.*
>
> *"Lorsque l'auteur est connu et domicilié en Belgique, l'éditeur, l'imprimeur ou le distributeur ne peut être poursuivi".*

Cet article a une grande importance car il détermine l'ordre dans lequel les responsabilités pénales et civiles doivent être imputées aux différents acteurs. En premier lieu, il faut citer l'auteur des faits, préciser s'il est connu et domicilié en Belgique. À défaut, la victime pourra citer l'éditeur, puis l'imprimeur et enfin le distributeur.

Cependant, il n'y a pas d'activité d'imprimeur ou de distributeur sur le net. La fonction d'éditeur est remplie par l'internaute. Pour que cet article soit applicable à internet, il faut que le délit de presse soit applicable sur la toile. Nous avons déjà abordé cette question dans le chapitre 4, sous-section 3.4 et nous savons donc que le délit de presse s'applique sur le net.

Il faut noter que la responsabilité en cascade ne remplace nullement les règles de responsabilité des prestataires définies par la loi du 15 décembre 2013. Mais le problème posé par la coexistence des deux systèmes de responsabilité n'a pas encore été tranché par la jurisprudence.

La doctrine estime que "*l'application de la responsabilité en cascade conduirait à retenir la responsabilité de plein droit d'un fournisseur de service du fait d'un contenu litigieux diffusé en ligne et permettrait ainsi de contourner le régime spécifique de responsabilité. Pour cette raison, elle doit être exclue, selon nous, pour*

autant que l'on se trouve dans les conditions d'application d'une exonération de responsabilité, en particulier celle d'une intervention passive"[64].

En d'autres termes, si le prestataire se trouve dans l'un des cas d'exonération que nous avons développés, la responsabilité en cascade ne doit pas s'appliquer.

Par contre, la responsabilité en cascade pourra s'appliquer si le prestataire ne remplit pas les conditions d'exonération de responsabilité. Dans ce cas, on revient au principe de l'article 1382 du Code civil. Or, lorsque l'on applique l'article 1382 du Code civil, la responsabilité en cascade s'applique et permet au prestataire de ne pas être poursuivi si l'auteur est connu et domicilié en Belgique.

Le tribunal de première instance de Bruxelles a rendu un jugement le 23 janvier 2007 allant dans ce sens: "*le privilège de pouvoir se soustraire à toute responsabilité, tant pénale que civile, lorsque l'auteur est connu et domicilié en Belgique, s'applique quelles que soient la nature, l'ampleur, la présentation ou le mode de publication opérés par la presse. Un rédacteur professionnel ou amateur, régulier ou occasionnel, écrivant sur support papier ou sur support informatique sera soumis aux mêmes droits et obligations. Le gestionnaire d'un site internet sur lequel sont publiés des articles doit en être considéré comme l'éditeur et bénéficier à ce titre du principe de responsabilité en cascade*"[65].

En d'autres mots, lorsque l'auteur est connu et domicilié en Belgique, l'éditeur bénéficie du principe de responsabilité en cascade et ne peut pas être poursuivi.

2.5 AUTRE CAS: LES FOURNISSEURS D'OUTILS DE RECHERCHE

Ces fournisseurs, ne bénéficiant pas d'un régime d'exonération, sont soumis au droit commun de la responsabilité. En revanche, le problème de la responsabilité des fournisseurs d'outils de recherche n'est pas encore réglé par le droit belge ou une directive européenne.

[64] CALLEWAERT, V., DE CONINCK, B., DUBUISSON, B., GATHEM, G., Section 2 - Les responsabilités sur internet, Bruxelles, Éditions Larcier, 2009, p. 1046-1059.
[65] Civ. Bruxelles (14e ch.), 23 janvier 2007, A&M, 2008/1, p. 78-83.

Tout d'abord, il existe deux outils de recherche sur la toile, les moteurs de recherche et les annuaires.

2.5.1 Le moteur de recherche

Wery E. définit le moteur de recherche comme "*un logiciel d'exploration, appelé "robot", qui visite en continu les pages web et les indexe de manière automatique dans une base de données, en fonction des mots-clés qu'ils contiennent*"[66]. En raison de l'automatisation, seul le filtre par mot-clé offensant empêche les contenus illicites lors du référencement. Cette protection est fragile. En effet, le site présentant du contenu illicite ne contenant pas de mot-clé repris par le filtre sera diffusé partout sur la toile.

C'est l'article 1382 du Code civil qui s'applique. La victime qui invoque la responsabilité d'un fournisseur d'outils de recherche devra prouver une faute de ce fournisseur en lien causal avec le dommage qu'elle a subi. Mais de quelle faute pourrait-on imputer le fournisseur d'outils de recherche? La seule faute possible serait que les fournisseurs d'outils de recherche soient au courant du caractère illégal des contenus qu'ils référencent mais qu'ils ne font rien pour les retirer ou en bloquer l'accès. Ce critère nous ramène à la "connaissance effective" que doit avoir l'hébergeur pour que sa responsabilité soit mise en cause.

2.5.2 Les annuaires

Il s'agit "*des répertoires de sites classés par thèmes, en catégories et sous-catégories de plus en plus précises, au sein desquelles s'affichent des listes de liens hypertextes renvoyant vers des sites internet*"[67].

À la différence des moteurs de recherche, les annuaires traitent la demande d'indexation des titulaires de site qui ont proposé une catégorie où placer leur site. En matière de responsabilité, l'annuaire se distingue du moteur de recherche par

[66] VERBIEST, T., Wery, E., "La responsabilité des fournisseurs d'outils de recherche et d'hyperliens du fait du contenu des sites référencés", *Droit & technologie,* le 11 septembre 2002 (Disponible sur: *http://www.droit-technologie.org/dossier-76/la-responsabilite-des-fournisseurs-d-8217-outils-de-recherche-et-d-8.html; consulté le 27 octobre 2014).*

[67] PIRLOT DE CORBION, S., "La responsabilité des fournisseurs d'outils de recherche sur Internet", D.A.O.R., 2004/4, n° 72, p. 12

le premier référencement où les annuaires doivent vérifier le contenu avant de le placer dans une catégorie, sinon il commet une faute.

Nous pensons qu'il serait utile que le législateur belge étende l'exonération des hébergeurs aux fournisseurs d'outils de recherche pour deux raisons:

Premièrement, d'autres pays comme l'Espagne, les États-Unis et d'autres pays européens ont déjà exonéré les fournisseurs d'outils de recherche. Or, la directive sur le commerce électronique a été prise dans le but d'harmoniser les législations dans les différents États afin d'éviter des divergences de législation.

Deuxièmement, les moteurs de recherche n'ont aucun contrôle sur les sites qu'ils référencent, tout comme les hébergeurs puisque les moteurs de recherche indexent automatiquement les pages. Or, il me paraît discriminatoire de traiter différemment ces deux types de prestataires.

CONCLUSION

Le terme "cybercriminalité" est une notion difficile à définir; il désigne l'ensemble des infractions pénales qui peuvent être commises par le bais d'un système informatique. Ces infractions regroupent quatre catégories d'infractions dont celle liée aux contenus illicites. Toutefois, un contenu sur internet est avant tout l'expression d'une pensée protégée par la liberté d'expression. Cette couverture légale derrière laquelle se cachent beaucoup d'auteurs de contenus portant préjudice aux droits d'autrui n'est pas absolue. Les États ont pris les dispositions pénales dans leurs lois nationales dans le but d'équilibrer le droit personnel à la liberté d'expression et le respect des droits d'autrui dans chaque État. En d'autres mots, les victimes de contenus illicites sur le net peuvent obtenir réparation pour des contenus sur internet qui vont à l'encontre de leurs droits.

En matière pénale, les délits commis sur internet peuvent être poursuivis en Belgique si l'un des éléments constitutifs de l'infraction a lieu sur le sol belge. Ces délits rassemblent une grande variété de contenus comme la pédopornographie, les propos racistes et xénophobes, la diffamation et la calomnie, le cyberharcèlement et également le délit de presse sur la toile. Dans tous les cas, les lois belges ont dû faire l'objet d'une interprétation extensive ou téléologique afin d'être applicables à internet. Du côté de la responsabilité civile, l'article 1382 du Code civil règle la question de la réparation du dommage causé sur le net, bien que cet article soit imprécis et qu'il implique que la victime doit démontrer une faute en lien causal avec son dommage pour pouvoir exiger une réparation de l'auteur ou des prestataires de service. De plus, Les prestataires exerçant une activité de simple transport, d'hébergement ou de stockage temporaire bénéficient d'une exonération sous certaines conditions.

La Belgique possède un arsenal juridique de taille qui manque cependant de précision quant à son application et de ce fait, cet arsenal s'oppose au principe de stricte interprétation du droit pénal. Pour ma part, je trouve que le législateur belge a encore beaucoup de travail pour lutter contre la cybercriminalité. Il devrait apporter des précisions pour que les articles du Code pénal s'appliquent sans ambiguïté

à internet, plutôt que de laisser la doctrine et la jurisprudence se diviser entre deux interprétations. En matière de pédopornographie, il a pris une mesure très efficace en permettant de sanctionner le simple consommateur afin que le marché de la pédopornographie s'écroule puisque, sans consommateur, les auteurs n'ont plus de revenu et plus aucune raison de diffuser la pédopornographie. L'absence de normes en la matière crée une insécurité juridique pour les délits commis sur le réseau, alors qu'il n'y aurait plus d'équivoque en rajoutant des dispositions propres à internet dans les lois belges. La compétence du tribunal correctionnel devrait également être étendue en ce qui concerne le délit de presse par lequel sont tenus des propos diffamatoires, car la procédure en cour d'assises est trop lourde à supporter pour les victimes.

De plus, le législateur devrait préciser davantage la responsabilité des prestataires de service pour garantir une certaine sécurité juridique et éviter que ceux-ci se retrouvent les premiers juges de contenus litigieux, alors qu'il appartient aux juridictions de qualifier un contenu sur internet contraire à la légalité. Pour cela, il conviendrait que le législateur prenne une norme autre que l'article 1382 du Code civil pour définir la responsabilité sur internet. Cette norme pourrait être rédigée comme suit:

> *Article 1382bis du Code civil: l'article 1382 du Code civil s'applique aux prestataires d'internet s'ils ne retirent pas ou ne bloquent pas l'accès au contenu manifestement illicite alors qu'ils ont la connaissance effective du caractère illicite de ce contenu.*

Le législateur devrait également étendre le régime applicable à l'hébergeur aux prestataires fournissant des outils de recherche.

Pour aller plus loin, la Belgique s'est dotée d'un centre pour la cybersécurité qui aura notamment pour tâche de proposer des améliorations du cadre légal. Il serait intéressant de savoir si le législateur profitera de la création de ce centre pour clarifier les normes existantes. Mais la vraie question est la suivante: quels changements le centre pour la cybersécurité va-t-il entreprendre pour tous les citoyens victimes des contenus illicites sur la toile?

BIBLIOGRAPHIE

1 DOCTRINE

BLAISE, N., "L'interdiction de consulter des images pédopornographiques sur internet: avancée ou précision?", *R.D.T.I.*, 2011/3, n° 44, p. 29-34.

BOUBKIRA, I., "La charge de la preuve en matière de discrimination", *J.D.J.*, 2011/8, n° 308, p. 20-28.

CALLEWAERT, V., DE CONINCK, B., DUBUISSON, B., GATHEM, G., *Section 2 - Les responsabilités sur internet*, Bruxelles, Larcier, 2009, p. 1046-1059.

CASSART, A., "L'extension de la notion de communauté d'intérêts aux réseaux sociaux", *R.D.T.I.*, 2013/3, n° 52, p. 101-106.

DE PATOUL, F., VEREECKEN, I., "La responsabilité des intermédiaires de l'internet: première application de la loi belge", R.D.T.I., 2004/2, p. 54.

DEBILIO, R., "Quand Internet s'invite dans la jurisprudence de la Cour de cassation: l'élément matériel du délit de presse se précise", *R.D.T.I.*, 2013/1, n° 50, p. 83-92.

DOCQUIR, P.-F., "Contrôle des contenus sur Internet et liberté d'expression au sens de la Convention européenne des droits de l'homme", *C.D.P.K.*, 2002, p. 173 à 193.

DONY, C., "La presse, une notion que le Constituant tarde à (re)définir ...", J.L.M.B., 2010/3, p. 137-142.

KER, C., "«Presse» ou «tribune électronique»: censure et responsabilité", *R.D.T.I.*, 2007/2, n° 28, p. 147-170.

LÉONARD, T., "L'exonération de responsabilité des intermédiaires en ligne: un état de la question", J.T., 2012/40-41, n° 6500, p. 814-818.

Livre vert de la Commission du 16 octobre 1996 sur la protection des mineurs et de la dignité humaine dans les services audiovisuels et d'information, C.O.M. (96) 483 final, p. 7.

PIRLOT DE CORBION, S., "La responsabilité des fournisseurs d'outils de recherche sur Internet", D.A.O.R., 2004/4, n° 72, p. 12.

POULLET, Y., *La lutte contre le racisme et la xénophobie sur l'internet*, J.T., 2006/23, n° 6229, p. 401-412.

STROWEL, A., IDE, N. et VERHOESTRAETE, F., "La directive du 8 juin 2000 sur le commerce électronique: un cadre juridique pour l'Internet", J.T., 2001/7, n° 6000, p. 133-145.

VALCKE, P., UYTTENDAELE, C., "Racisme et négationnisme sur l'Internet: les affaires Infonie et Yahoo! Bis", *R.D.T.I.*, 2002/2, p. 87.

VAN CANNEYT, T., VERDURE, C., "La validité des constats d'huissier relatifs à des sites internet", *R.D.T.I.*, 2009/1, n° 34, p. 47-57.

VAN ENIS, Q., *Le délit de presse sur internet: la cohérence et rien de plus?*, J.T., 2009/3, n° 6337, p. 48-50.

VERBIEST, T., WERY, E., "La responsabilité des fournisseurs d'outils de recherche et d'hyperliens du fait du contenu des sites référencés", *Droit & technologie,* le 11 septembre 2002 (Disponible sur: *http://www.droit-technologie.org/dossier-76/la-responsabilite-des-fournisseurs-d-8217-outils-de-recherche-et-d-8.html;* consulté le 27 octobre 2014).

VERBIEST, T., WERY, E., *La Responsabilité des fournisseurs de services internet: derniers développements jurisprudentiels*, J.T., 2001, p. 165-173.

WÉRY, E., "Internet hors la loi? Description et introduction à la responsabilité des acteurs du réseau", J.T., 1997, p. 419.

WERY, E., "La visualisation de pornographie enfantine est-elle punissable?", *Droit & technologie*, le 1er août 2011 [en ligne]. (Disponible sur: http://www.droit-technologie.org/actuality-1422/la-visualisation-de-pornographie-enfantine-est-elle-punissable.html; consulté le 21 juillet 2014).

2 JURISPRUDENCE

Comm. Bruxelles, 2 novembre 1999, A. & M., 2000, p. 474.

Civ. Bruxelles (réf.), 2 mars 2000, n° 6042, *J.T.*, 2002/6, p. 113-116.

Cass., 3 février 2004, n° F-20040203-3, inédit (disponible sur www.juridat.be; consulté le 27 octobre 2014).

Cass., (2e ch.), 3 février 2004, R.D.T.I., 2004/2, p. 51.

Cass., (1re ch.), 2 juin 2006, Pas., 2006/5-6, p. 1302.

Civ. Bruxelles (14e ch.), 23 janvier 2007, A&M, 2008/1, p. 78-83.

Mons, 14 mai 2008, n° F-20080514-1, inédit (disponible sur, www.juridat.be; consulté le 27 octobre 2014).

Corr. Bruxelles (54ème ch.), 23 juin 2009, *J.L.M.B.*, 2010/3, p. 123-127.

Corr. Bruxelles (61ème ch.), 27 novembre 2009, J.L.M.B., 2010/1, p. 10-17.

Civ. Anvers (5ème ch. B), 3 décembre 2009, 09/1322/A, *A. & M.*, 2010/5-6, p. 560-562.

Cass., (2ème ch.), 20 avril 2011, P.10.2006.F, R.D.T.I., 2011/3, n° 44, p. 27-28.

C.C., 22 décembre 2011, n° 198/2011, © Cour constitutionnelle de Belgique, 25/04/2012, (disponible sur www.const-court.be; consulté le 15 mars 2015).

Corr. Bruxelles (chambre du conseil), 14 février 2012, *J.L.M.B.*, 2012/17, p. 817-819.

Cass., 6 mars 2012, J.T., 2012, p. 505.

Cass., (2ème ch.), 29 octobre 2013, *J.T.*,2014/21, n° 6565, p. 391-392.

3 JURISPRUDENCE EUROPÉENNE

Cour eur. D. H., (6538/74) - Cour (Plénière) - Arrêt (au principal) - AFFAIRE SUNDAY TIMES c. ROYAUME-UNI (N° 1) © Hudoc, 26/04/1979, (disponible sur http://hudoc.echr.coe.int/; consulté le 23 mars 2015).

Cour eur. D. H., Arrêt Prager et Oberschlick contre Autriche du 26 avril 1995, série A n° 313, p. 18, § 37, p. 19, § 38

Cour eur. D. H., Arrêt Fressoz et Roire contre France du 21 janvier 1999, n° 29183/95.

Cour eur. D. H., Arrêt Roy et Malaurie contre France du 3 Octobre 2000, n° 34000/96.

4 LÉGISLATION BELGE

C. civ., art. 1382.

C. pén., art. 383bis. §1, §2.

C. pén., art. 442bis. al. 1, al. 3.

C. pén., art. 443. al. 1er.

C. pén., art. 444.

Const., art. 19.

Const., art. 22.

Const., art. 25.

Const., art. 150.

L. du 13 juin 2005 relative aux communications électroniques, art. 145. §3bis, *M.B.*, 20 juin 2005, p. 28070.

L. du 15 décembre 2013 portant insertion du Livre XII, " Droit de l'économie électronique " dans le Code de droit économique, portant insertion des définitions propres au Livre XII et des dispositions d'application de la loi propres au Livre XII, dans les Livres I et XV du Code de droit économique, art. XII.17, XII.18, XII.19, XII.20, *M.B.*, 14 janvier 2014, p. 1524.

L. du 28 novembre 2000 relative à la criminalité informatique, art. 550bis, 550ter, 504quater, *M.B.*, 3 février 2001, p. 02909.

L. du 30 juillet 1981 tendant à réprimer certains actes inspirés par le racisme ou la xénophobie, art. 20, 21, 22, 30, *M.B.*, 8 août 1981, p. 9928.

5 LÉGISLATION EUROPÉENNE

Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales telle qu'amendée par les Protocoles n° 11 et n° 14 signée à Rome le 4 novembre 1950 et approuvée par la loi du 14 juin 1955 (Disponible sur: http://conventions.coe.int/treaty/fr/Treaties/Html/005.htm; consulté le 27 octobre 2014).

Convention sur la cybercriminalité signée à Budapest le 23 novembre 2001 et approuvée par la loi du 20 août 2012 (Disponible sur http://www.conventions.coe.int/Treaty/fr/Treaties/Html/185.htm; consulté le 15 juillet 2014).

Directive (CE) n° 2000/31 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), J.O.C.E., n° L 178 du 17 juillet 2000, p. 1.

6 SITES INTERNET/IMAGES

DEMOULIN Marie, HEIRMAN Wannes, VAN DER PERRE Aurélie, WALRAVE Michel, "Cyberharcèlement: risque du virtuel, impact dans le réel", *internet-observatory.be* [en ligne]. Disponible sur www.internet-

observatory.be/internet.../pdf/.../Boek_cyberpesten_fr.pdf (consulté le 1 décembre 2014).

FRICHET, Thibaud. Schema identification [image PNG]. In FRICHET, Thibaud. *Anonymat sur Internet: Point sur la situation* [en ligne]. FRICHET, Thibaud, 2013. Disponible sur: <http://blog.tfrichet.fr/wp-content/uploads/2013/06/Schema-identification-user.png> (consulté le 6 avril 2015).

http://securityresponse.symantec.com/fr/be/norton/cybercrime/definition.jsp (consulté le 18 novembre 2014)

http://www.larousse.fr/dictionnaires/francais/cybercriminalit%C3%A9/10910062 (consulté le 18 novembre 2014)

http://www.larousse.fr/dictionnaires/francais/num%C3%A9rique/55253 (consulté le 30 janvier 2015)

http://www.larousse.fr/dictionnaires/francais/racisme/65932 (consulté le 18 novembre 2014)

http://www.larousse.fr/dictionnaires/francais/x%C3%A9nophobie/82881 (consulté le 18 novembre 2014)

KASPERSKY-LAB. The risk of infection during Internet surfing in North America and Western Europe in the first half of 2012 [image PNG]. In KASPERSKY-LAB. *The geography of cybercrime: Western Europe and North America: Substituting search results* [en ligne]. Yury Namestnikov, 2012. Disponible sur: <http://www.viruslist.com/fr/images/vlill/namest_sept2012_pic08.png> (consulté le 6 avril 2015).

NARKCRY.Parte visible de internet. [image PNG]. In NARKCRY. *Mi experiencia en la Deep Web o Internet Profundo*. [en ligne]. NARKCRY, 2014. Disponible sur: <http://pills52.com/upload/9/05/905d82ee9960276d_thumb.jpg> (consulté le 6 avril 2015).

SIMARD, Eric. Dos attack schema [image PNG]. In SIMARD, Eric. *Protecting Your DNS Server Against DDoS Attacks* [en ligne]. GLOBOTECH COMMUNICATIONS, 2014. Disponible sur: <http://www.gtcomm.net/blog/wp-content/uploads/2014/02/dos-attack-schema.jpg> (consulté le 6 avril 2015).

THE TOR PROJECT, INC. Tor circuit step three [image PNG]. In THE TOR PROJECT, INC. *Tor: Overview: The solution: a distributed, anonymous network* [en

ligne]. THE TOR PROJECT, INC. Disponible sur: <https://www.torproject.org/images/htw3.png> (consulté le 6 avril 2015).

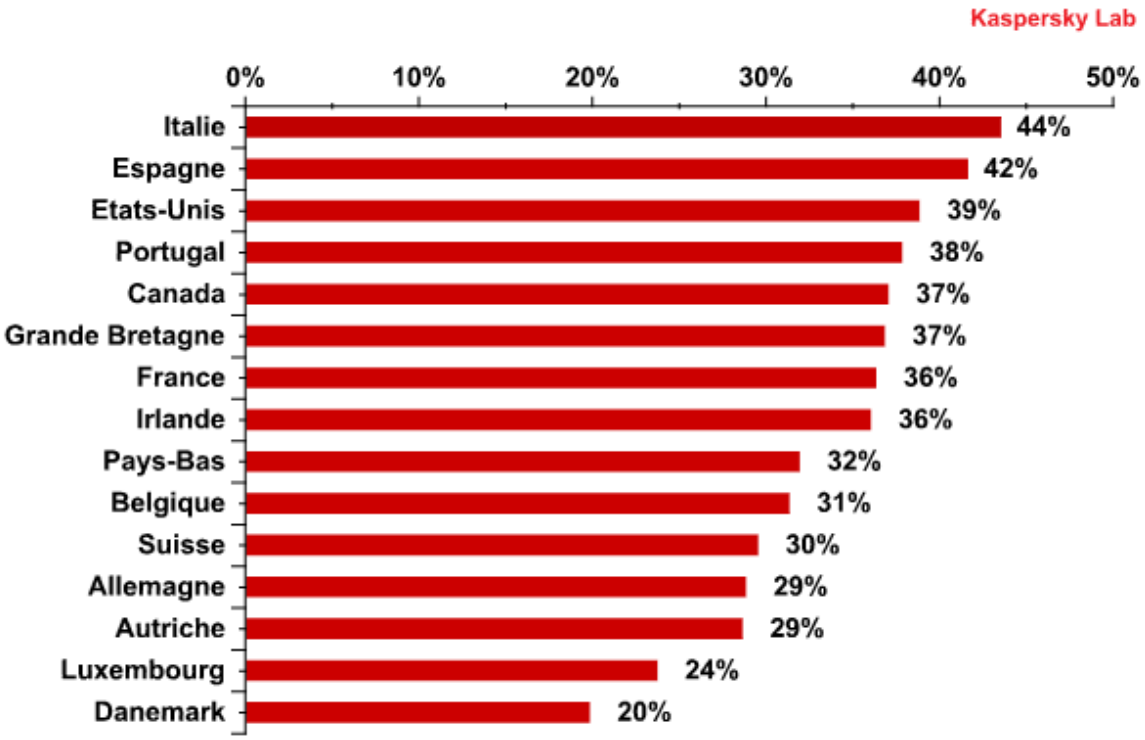
V. KAISER, "La protection des mineurs sur Internet: la problématique de la pédo-pornographie et des contenus jugés préjudiciables", 2010. Disponible sur http://www.fundp.ac.be/droit/dtic/publications.html; (consulté le 7 juillet 2014).

TABLE DES MATIÈRES

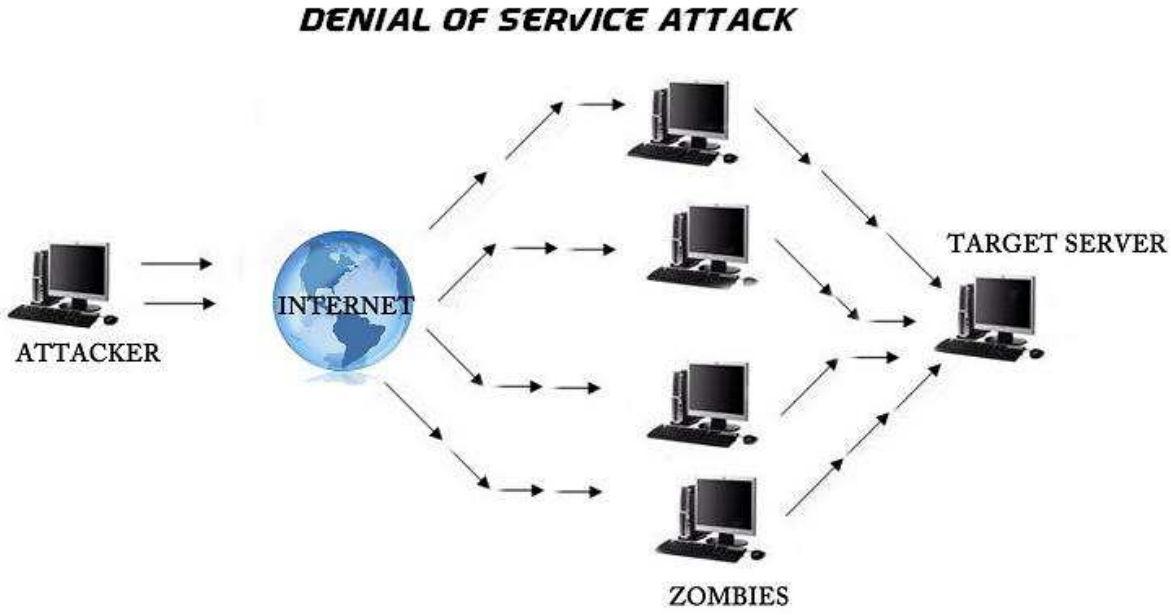
LISTE DES ANNEXES

ANNEXES

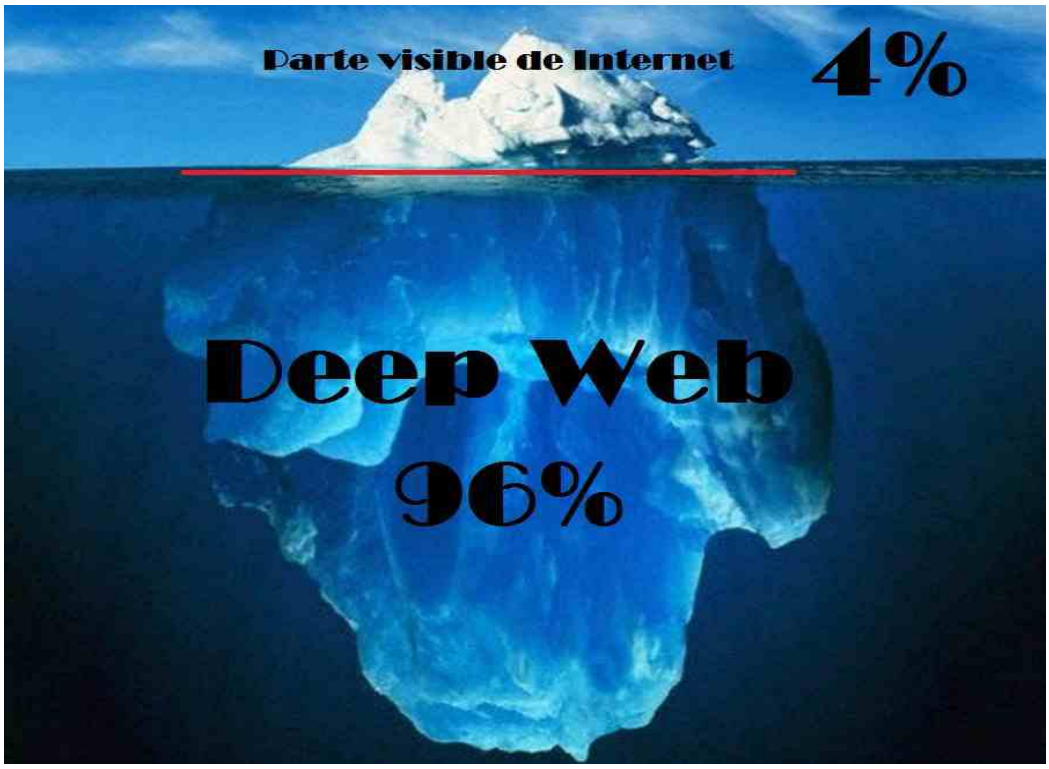
Annexe 1



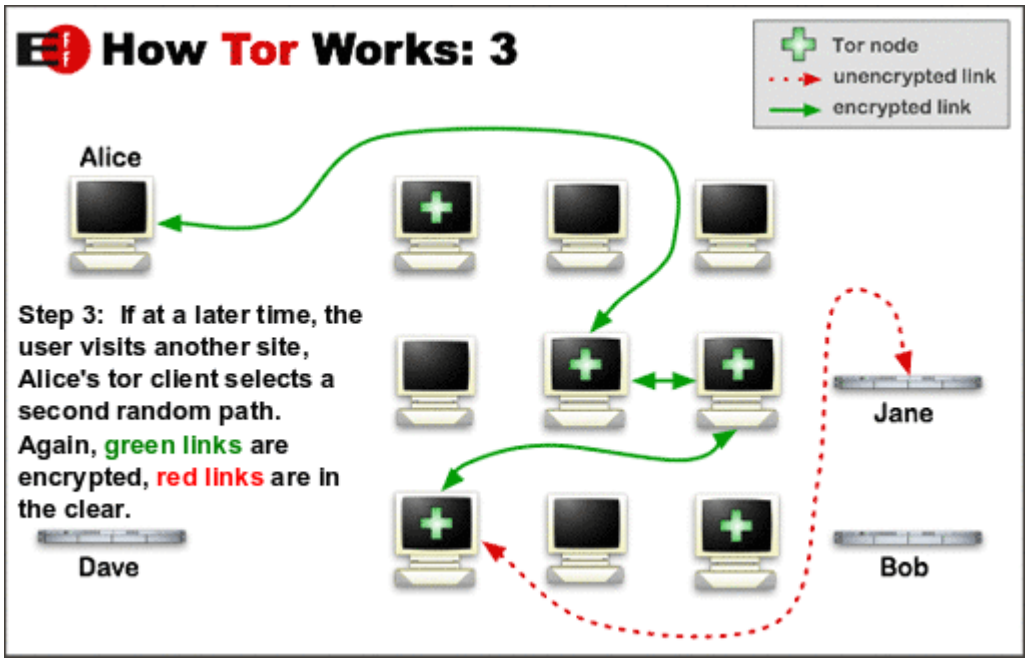
Annexe 2



Annexe 3



Annexe 4



Annexe 5

Convention sur la cybercriminalité
STCE no. : 185
Traité ouvert à la signature des Etats membres et des Etats non membres qui ont participé à son élaboration et à l'adhésion des autres Etats non membres

Ouverture à la signature
Lieu : Budapest
Date : 23/11/2001

Entrée en vigueur
Conditions : 5 Ratifications incluant au moins 3 Etats membres du Conseil de l'Europe
Date : 1/7/2004

Situation au 14/5/2015

Etats membres du Conseil de l'Europe

	Signature	Ratification	Entrée en vigueur	Renv.	R.	D.	A.	T.	C.	O.
Albanie	23/11/2001	20/6/2002	1/7/2004				X			
Allemagne	23/11/2001	9/3/2009	1/7/2009		X	X	X			
Andorre	23/4/2013									
Arménie	23/11/2001	12/10/2006	1/2/2007				X			
Autriche	23/11/2001	13/6/2012	1/10/2012		X	X	X			
Azerbaïdjan	30/6/2008	15/3/2010	1/7/2010		X	X	X	X		
Belgique	23/11/2001	20/8/2012	1/12/2012		X	X	X			
Bosnie-Herzégovine	9/2/2005	19/5/2006	1/9/2006				X			
Bulgarie	23/11/2001	7/4/2005	1/8/2005		X	X	X			
Chypre	23/11/2001	19/1/2005	1/5/2005				X			
Croatie	23/11/2001	17/10/2002	1/7/2004				X			
Danemark	22/4/2003	21/6/2005	1/10/2005		X		X	X		
Espagne	23/11/2001	3/6/2010	1/10/2010			X	X			
Estonie	23/11/2001	12/5/2003	1/7/2004				X			
Finlande	23/11/2001	24/5/2007	1/9/2007		X	X	X			
France	23/11/2001	10/1/2006	1/5/2006		X	X	X			
Géorgie	1/4/2008	6/6/2012	1/10/2012			X				
Grèce	23/11/2001									
Hongrie	23/11/2001	4/12/2003	1/7/2004		X	X	X			
Irlande	28/2/2002									
Islande	30/11/2001	29/1/2007	1/5/2007		X		X			
Italie	23/11/2001	5/6/2008	1/10/2008				X			
Lettonie	5/5/2004	14/2/2007	1/6/2007		X		X			
L'ex-République yougoslave de Macédoine	23/11/2001	15/9/2004	1/1/2005				X			
Liechtenstein	17/11/2008									
Lituanie	23/6/2003	18/3/2004	1/7/2004		X	X	X			
Luxembourg	28/1/2003	16/10/2014	1/2/2015				X			
Malte	17/1/2002	12/4/2012	1/8/2012			X				
Moldova	23/11/2001	12/5/2009	1/9/2009			X	X	X		
Monaco	2/5/2013									
Monténégro	7/4/2005	3/3/2010	1/7/2010	55	X		X			
Norvège	23/11/2001	30/6/2006	1/10/2006		X	X	X			
Pays-Bas	23/11/2001	16/11/2006	1/3/2007				X	X		
Pologne	23/11/2001	20/2/2015	1/6/2015		X		X			
Portugal	23/11/2001	24/3/2010	1/7/2010			X	X			
République tchèque	9/2/2005	22/8/2013	1/12/2013		X	X	X			
Roumanie	23/11/2001	12/5/2004	1/9/2004				X			
Royaume-Uni	23/11/2001	25/5/2011	1/9/2011		X		X			
Russie										
Saint-Marin										
Serbie	7/4/2005	14/4/2009	1/8/2009	55			X			
Slovaquie	4/2/2005	8/1/2008	1/5/2008		X	X	X			
Slovénie	24/7/2002	8/9/2004	1/1/2005				X			
Suède	23/11/2001									
Suisse	23/11/2001	21/9/2011	1/1/2012		X	X	X			
Turquie	10/11/2010	29/9/2014	1/1/2015							
Ukraine	23/11/2001	10/3/2006	1/7/2006		X		X			

Non membres du Conseil de l'Europe

	Signature	Ratification	Entrée en vigueur	Renv.	R.	D.	A.	T.	C.	O.
Afrique du Sud	23/11/2001									
Argentine										
Australie		30/11/2012 a	1/3/2013		X		X			
Canada	23/11/2001									
Chili										
Colombie										
Costa Rica										
Etats-Unis d'Amérique	23/11/2001	29/9/2006	1/1/2007		X	X	X			

Israël										
Japon	23/11/2001	3/7/2012	1/11/2012		X	X	X			
Maroc										
Maurice		15/11/2013 a	1/3/2014				X			
Mexique										
Panama		5/3/2014 a	1/7/2014				X			
Paraguay										
Pérou										
Philippines										
République dominicaine		7/2/2013 a	1/6/2013			X	X			
Sénégal										
Sri Lanka										
Tonga										

Nombre total de signatures non suivies de ratifications :	8
Nombre total de ratifications/adhésions :	45

Renvois :
(55) Date de signature par l'union d'état de Serbie-Monténégro.
a.: Adhésion - s.: Signature sans réserve de ratification - su.: Succession - r.: signature "ad referendum".
R.: Réserves - D.: Déclarations - A.: Autorités - T.: Application territoriale - C.: Communication - O.: Objection.

Source : Bureau des Traités sur http://conventions.coe.int – * Disclaimer

Annexe 6

Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques
STCE no. : 189
Traité ouvert à la signature des Etats qui ont signé le Traité STE 185

Ouverture à la signature
Lieu : Strasbourg
Date : 28/1/2003

Entrée en vigueur
Conditions : 5 Ratifications.
Date : 1/3/2006

Situation au 14/5/2015

Etats membres du Conseil de l'Europe

	Signature	Ratification	Entrée en vigueur	Renv.	R.	D.	A.	T.	C.	O.
Albanie	26/5/2003	26/11/2004	1/3/2006							
Allemagne	28/1/2003	10/6/2011	1/10/2011							
Andorre	23/4/2013									
Arménie	28/1/2003	12/10/2006	1/2/2007							
Autriche	30/1/2003									
Azerbaïdjan										
Belgique	28/1/2003									
Bosnie-Herzégovine	9/2/2005	19/5/2006	1/9/2006							
Bulgarie										
Chypre	19/1/2005	23/6/2005	1/3/2006							
Croatie	26/3/2003	4/7/2008	1/11/2008		X					
Danemark	11/2/2004	21/6/2005	1/3/2006		X			X		
Espagne	27/11/2013	18/12/2014	1/4/2015			X				
Estonie	28/1/2003									
Finlande	28/1/2003	20/5/2011	1/9/2011		X					
France	28/1/2003	10/1/2006	1/5/2006			X				
Géorgie										
Grèce	28/1/2003									
Hongrie										
Irlande										
Islande	9/10/2003									
Italie	9/11/2011									
Lettonie	5/5/2004	14/2/2007	1/6/2007							
L'ex-République yougoslave de Macédoine	14/11/2005	14/11/2005	1/3/2006							
Liechtenstein	17/11/2008									
Lituanie	7/4/2005	12/10/2006	1/2/2007			X				
Luxembourg	28/1/2003	16/10/2014	1/2/2015							
Malte	28/1/2003									
Moldova	25/4/2003									
Monaco										
Monténégro	7/4/2005	3/3/2010	1/7/2010	55	X					
Norvège	29/4/2008	29/4/2008	1/8/2008		X					
Pays-Bas	28/1/2003	22/7/2010	1/11/2010		X			X		
Pologne	21/7/2003	20/2/2015	1/6/2015		X					
Portugal	17/3/2003	24/3/2010	1/7/2010							
République tchèque	17/5/2013	7/8/2014	1/12/2014							
Roumanie	9/10/2003	16/7/2009	1/11/2009		X					
Royaume-Uni										
Russie										
Saint-Marin										
Serbie	7/4/2005	14/4/2009	1/8/2009	55						
Slovaquie										
Slovénie	26/2/2004	8/9/2004	1/3/2006							
Suède	28/1/2003									
Suisse	9/10/2003									
Turquie										
Ukraine	8/4/2005	21/12/2006	1/4/2007			X				

Non membres du Conseil de l'Europe

	Signature	Ratification	Entrée en vigueur	Renv.	R.	D.	A.	T.	C.	O.
Afrique du Sud	4/4/2008									
Argentine										
Australie										
Canada	8/7/2005									
Chili										
Colombie										
Costa Rica										
Etats-Unis d'Amérique										

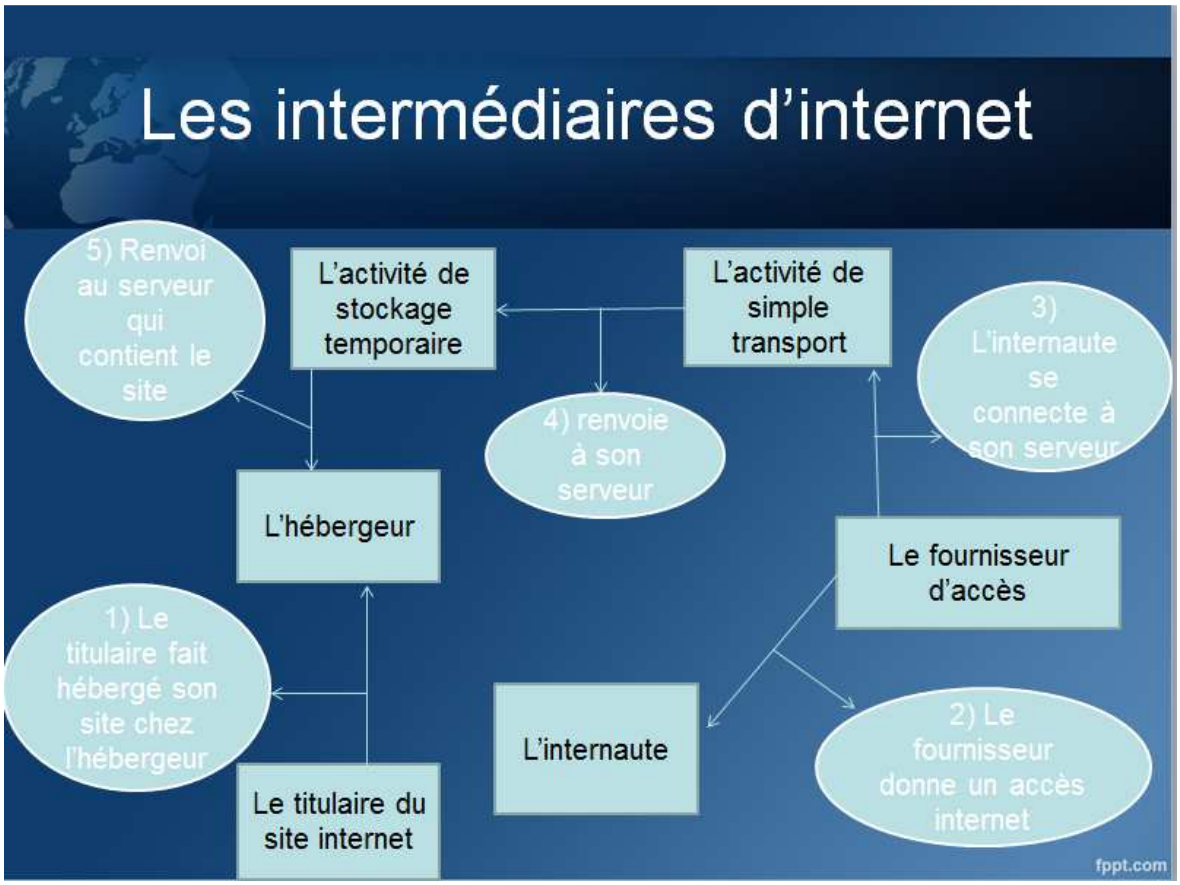
Israël										
Japon										
Maroc										
Maurice										
Mexique										
Panama										
Paraguay										
Pérou										
Philippines										
République dominicaine										
Sénégal										
Sri Lanka										
Tonga										

Nombre total de signatures non suivies de ratifications :	14
Nombre total de ratifications/adhésions :	24

Renvois :
(55) Date de signature par l'union d'état de Serbie-Monténégro.
a.: Adhésion - s.: Signature sans réserve de ratification - su.: Succession - r.: signature "ad referendum".
R.: Réserves - D.: Déclarations - A.: Autorités - T.: Application territoriale - C.: Communication - O.: Objection.

Source : Bureau des Traités sur http://conventions.coe.int – * Disclaimer

Annexe 7



Annexe 8