

Faculté de droit et de criminologie

La traite des êtres humains à l'ère numérique : Internet au service de l'exploitation sexuelle

Dans quelle mesure le droit pénal et le droit de la procédure pénale répondent-ils efficacement à ce phénomène ?

Auteur : Elise Charlier
Promoteur : Daniel Flore
Année académique 2020-2021
Master en droit – Justice civile et pénale

Plagiat et erreur méthodologique grave

Le plagiat, fût-il de texte non soumis à droit d'auteur, entraîne l'application de la section 7 des articles 87 à 90 du règlement général des études et des examens.

Le plagiat consiste à utiliser des idées, un texte ou une œuvre, même partiellement, sans en mentionner précisément le nom de l'auteur et la source au moment et à l'endroit exact de chaque utilisation*.

En outre, la reproduction littérale de passages d'une œuvre sans les placer entre guillemets, quand bien même l'auteur et la source de cette œuvre seraient mentionnés, constitue une erreur méthodologique grave pouvant entraîner l'échec.

* A ce sujet, voy. notamment <http://www.uclouvain.be/plagiat>.

Remerciements

Tout d'abord je tiens à remercier mon promoteur, Daniel Flore pour son accompagnement bienveillant tout au long de la rédaction de ce mémoire.

Ensuite je remercie tous mes proches, pour le soutien qu'ils m'ont apporté non seulement au cours de la réalisation de ce mémoire mais également pendant tout mon parcours universitaire.

En particulier j'aimerais exprimer toute ma gratitude envers mes parents pour leurs précieux conseils et le temps qu'ils ont consacré à la relecture de ce mémoire.

Enfin, j'ai une pensée pour Seymour Dragh, une épaule solide sur laquelle j'ai toujours pu m'appuyer.

Table des matières

Introduction.....	1
Titre 0. Traite sexuelle et Internet : l'émergence d'un nouveau modus operandi	2
Chapitre I. La traite sexuelle, un cybercrime.....	2
Chapitre II. Le recrutement des victimes via Internet	2
Chapitre III. L'exploitation des victimes via Internet.....	3
Titre I. La traite sexuelle et Internet : incriminations et sanctions.....	5
Chapitre I. La traite des êtres humains	5
Section I. Le Protocole de Palerme des Nations Unies	5
Section II. La Convention du Conseil de l'Europe sur la lutte contre la traite des êtres humains	8
Section III. La directive de l'Union européenne sur la traite des êtres humains.....	10
Section IV. Le droit belge : L'article 433quinquies du Code pénal.....	11
§1 ^{er} . Éléments constitutifs	11
A. Éléments matériels.....	12
B. Éléments moraux.....	14
C. Clarifications quant à la nécessité d'une filière.....	18
§2. La peine.....	19
Chapitre II. La cyberprédation et le grooming	21
Section I. La cyberprédation	23
Section II. La sollicitation de mineurs à des fins sexuelles.....	25
Chapitre III. Publicité d'offre à caractère sexuel sur Internet et responsabilité des plateformes numériques	28
Section I. La publicité d'offres à caractère sexuel sur Internet.....	28
Section II. La responsabilité des prestataires intermédiaires.....	30
§1. Considérations préliminaires.....	30
§2. La directive e-commerce	31
§3. L'exonération de responsabilité des prestataires intermédiaires.....	31
A. Champ d'application.....	31
B. Conditions.....	32
C. En pratique.....	34
§4. D'hébergeur à éditeur : Le cas Vivastreet en France	35
§5. Les lois FOSTA/SESTA aux États-Unis : un exemple à suivre ou ne pas suivre ?	36
§6. Conclusion	37
Titre II. Les moyens d'enquête pour lutter contre l'usage d'Internet dans la traite à des fins d'exploitation sexuelle.....	39
Chapitre I. La recherche policière dans les sources ouvertes	39
Section I. Patrouiller sur Internet de manière proactive	39
§1. Sources ouvertes sur Internet.....	39
§2. L'enquête proactive	40
Section II. Cadre légal	40

§1. L'arrêt du 28 mars 2017 de la Cour de Cassation	40
§2. Lieu accessible au public dans un contexte numérique	41
§3. Conditions de mise en œuvre	42
§4. Un besoin de clarification.....	42
Section III. Recherche dans les sources ouvertes, observation et infiltration	43
§1. L'article 47sexies du Code d'instruction criminelle.....	43
§2. L'analyse à grande échelle de données publiques : légal ?	44
§3. L'infiltration sur Internet.....	45
Chapitre II. L'accès au contenu des smartphones des suspects et des victimes.....	46
Section I. La recherche locale (39bis, §2, C.I.Cr.).....	46
Section II. L'extension de recherche (88ter et 39bis, §5, C.I.Cr.).....	47
Chapitre III. La collaboration des fournisseurs de service à l'enquête pénale, un élément essentiel de la lutte contre la traite des êtres humains à l'ère numérique	50
Section I. L'insuffisance de l'entraide judiciaire internationale	50
Section II. Les obligations de collaboration des fournisseurs de services	52
§1. Mesures susceptibles de nécessiter la collaboration d'entreprises privées	52
A. L'article 46bis : L'identification des personnes publiant des offres à caractère sexuel liées à des faits de traite	52
B. L'article 88bis : Le repérage de communications électroniques ou la localisation de l'origine ou de la destination des communications électroniques entre le trafiquant et la victime	54
C. L'article 90ter : La prise de connaissance ou l'interception des communications entre le trafiquant et la victime	55
§2. Champ d'application personnel et territorial des obligations	58
A. Champ d'application personnel des obligations de collaboration	58
B. Champ d'application territorial des obligations de collaboration	60

Introduction

La traite des êtres humains est un crime particulièrement grave et une violation flagrante des droits fondamentaux, reconnue comme telle par la communauté internationale. Ce phénomène criminel grave est en constante évolution, dans un contexte de globalisation, de mobilité facilitée et de développement d'Internet et des nouvelles technologies. En 2016, Europol tirait la sonnette d'alarme : « L'évolution mondiale des infrastructures en ligne a fait d'Internet un outil crucial pour les trafiquants d'êtres humains, et il prendra probablement plus d'importance encore à l'avenir. Les interactions en ligne facilitent plusieurs facettes de la traite et de l'exploitation des êtres humains : l'identification de victimes potentielles, l'accès à des données à caractère personnel, l'organisation des aspects logistiques et de transport, le recrutement par le biais des réseaux sociaux, les forums de discussion et autres sites web, la publicité des victimes, leur exploitation et leur surveillance »¹.

Cette utilisation abusive d'Internet par les criminels constitue aujourd'hui une préoccupation et un défi pour les autorités répressives chargées de la lutte contre la traite des êtres humains. À l'heure où le droit pénal et le droit de la procédure pénale doivent sans cesse s'adapter aux nouvelles technologies de l'information et de la communication, ce travail a pour ambition d'évaluer l'état du droit belge, influencé par le droit européen et international, en rapport avec notre problématique qui est celle de la traite des êtres humains via Internet. Notre recherche sera centrée sur la traite des êtres humains à des fins d'exploitation sexuelle. Cette forme de traite est la plus répandue sur le territoire européen, et touche majoritairement des femmes et des filles de plus en plus jeunes. C'est également la forme d'exploitation dans laquelle l'usage d'Internet est le plus marqué.

Dans un premier temps, nous exposons brièvement les principaux usages qui sont fait d'Internet par les criminels dans le cadre de l'exploitation sexuelle de leurs victimes (Titre 0). Les différentes incriminations et sanctions qui s'appliquent à la problématique seront ensuite analysées (Titre I). Enfin, les moyens d'enquête disponibles aux autorités répressives belges seront passés en revue en fonction des différentes utilisations qui sont faites d'Internet par les trafiquants (Titre II).

¹ EUROPOL, *Trafficking in human beings in the EU*, Situation report, La Haye, février 2016, p.12 disponible sur : <https://www.europol.europa.eu/publications-documents/trafficking-in-human-beings-in-eu>.

Titre 0. Traite sexuelle et Internet : l'émergence d'un nouveau modus operandi

Chapitre I. La traite sexuelle, un cybercrime

Internet peut devenir l'outil de n'importe quel crime, qui devient alors un cybercrime, ce terme renvoyant à des infractions classiques mais fréquemment commises et facilitées par l'utilisation de réseaux électroniques. Ces cyber-délits sont commis « hors ligne » mais sont influencés par les technologies de l'information et de la communication². Tel est le cas de la traite des êtres humains à des fins d'exploitation sexuelle commise via des canaux numériques. Les groupes criminels organisés tirent grand avantage de cette utilisation, qui leur permet d'étendre leurs activités sur plusieurs pays et d'atteindre un niveau d'organisation jamais atteint auparavant. L'usage d'Internet aux fins d'exploitation sexuelle présente de nombreux avantages pour les trafiquants : rapidité, facilité d'utilisation, faible coût, anonymat, et difficulté de localiser les activités illicites. Tous ces éléments contribuent à générer un sentiment d'impunité chez les trafiquants, qui se sentent à l'abri dans le cyberspace.

Insistons sur le fait que la technologie n'est pas la cause des activités illicites des trafiquants, mais elle joue un rôle facilitant. Dans ce contexte, on assiste à l'émergence d'un nouveau « cyber modus operandi »³. La traite des êtres humains, que nous analysons en détail dans la suite de ce travail, se caractérise par une série d'étapes consécutives plutôt qu'en un comportement unique : recrutement, transport, contrôle, exploitation. Internet peut jouer un rôle à chacune de ces étapes⁴. Dans les cas d'exploitation sexuelle, deux phases sont par ailleurs particulièrement marquées par cet usage, celle du recrutement des victimes d'une part et celle de l'exploitation des victimes d'autre part.

Chapitre II. Le recrutement des victimes via Internet

Internet offre aux trafiquants un accès à un grand nombre de victimes potentielles. Il permet de recruter les victimes à distance, parfois sans jamais entrer réellement en contact avec elles, ce qui réduit le risque d'être repéré par les autorités répressives. Deux méthodes ressortent en ce

² F. DECHAMPS et C. LAMBILOT, *Cybercriminalité - État des lieux*, Limal, Anthémis, 2016, p.24.

³ S. RAETS et J. JANSSENS, « Trafficking and Technology: Exploring the Role of Digital Communication Technologies in the Belgian Human Trafficking Business », *European Journal on Criminal Policy and Research*, 2019. p. 6.

⁴ *Ibid.*

qui concerne le recrutement de victimes à des fins d'exploitation sexuelle sur Internet. D'une part les victimes peuvent être recrutées de manière indirecte au moyen d'annonces d'emploi trompeuses publiées sur Internet. D'autre part les trafiquants peuvent approcher directement les victimes via les réseaux sociaux ou autres plateformes d'échange de communications en ligne.

Les trafiquants utilisent des sites d'annonces d'offres d'emploi pour y publier des fausses annonces pour des emplois d'aide à domicile, de mannequinat, de danseuse, d'hôtesse, ou parfois directement des offres d'emploi dans le milieu de la prostitution⁵.

Les réseaux sociaux (Facebook, Instagram, Snapchat, sites de rencontres) sont également un moyen redoutable d'approcher des victimes car ceux-ci constituent de véritables « catalogues » sur lesquels les trafiquants peuvent trouver beaucoup d'informations sur les victimes (niveau d'éducation, liens familiaux, situation, lieu de résidence). Cet usage d'Internet est particulièrement dangereux pour les jeunes victimes, car celle-ci s'exposent plus largement sur les réseaux sociaux. Le recrutement à des fins d'exploitation sexuelle de jeunes personnes est souvent accompagné d'un processus de *grooming* destiné à gagner leur confiance et à les préparer à des abus sexuels. La technique du « *loverboy* » renvoie à celle qu'utilisent les trafiquants pour séduire la victime et créer chez elle un état de dépendance émotionnelle. Sur Internet, ce procédé prend moins de temps car le monde virtuel a tendance à créer un climat de confiance qui pousse la victime à abaisser ses barrières psychologiques plus rapidement. Les informations disponibles sur les réseaux sociaux peuvent être utilisées pour identifier les vulnérabilités des victimes, ce qui permet aux trafiquants d'affiner leur technique de recrutement et ainsi augmenter leurs chances de réussite.

Chapitre III. L'exploitation des victimes via Internet

Les trafiquants d'êtres humains considèrent les personnes comme des marchandises dont ils gèrent le marketing. C'est ainsi que, à des fins de profits, ils font la publicité des services de leur victime sur Internet afin d'attirer des clients pour ces services. Cette publicité se fait sur des sites accessibles à tous, car les trafiquants souhaitent que leurs annonces soient accessibles au plus grand nombre de clients. En matière d'exploitation sexuelle cela prend la forme d'offres

⁵ MYRIA, *Rapport annuel traite et trafic des êtres humains*, 2010, p. 115, disponible sur <https://www.myria.be/files/Traite-rapport-2010.pdf>.

de services de prostitution, sur des sites Internet qui sont par ailleurs également utilisés par les travailleurs du sexe. En effet, Internet a réellement bouleversé l'industrie de la prostitution puisqu'aujourd'hui la majorité de l'offre et de la demande de ce type de services s'est déplacée vers Internet, qui offre un cadre plus discret pour discuter des modalités d'une rencontre, pour les vendeurs comme pour les acheteurs. Les annonces qui offrent les services de victimes de traite se perdent alors dans la masse d'annonces à caractère prostitutionnel que l'on peut trouver sur Internet. Un rapport de Child Focus⁶ sur les proxénètes d'adolescents à Bruxelles indique qu'Internet est systématiquement utilisé dans le cadre de l'exploitation de victimes mineures. Les proxénètes utilisent des sites comme « Quartier Rouge », un site belge qui surfe sur le concept d'escorte. Dans ce type d'annonces, le nom et l'âge de la victime est modifié pour ne pas attirer l'attention. Plus encore qu'un moyen de faire la publicité des services des victimes, Internet peut devenir la modalité de leur exploitation⁷, lorsque les victimes sont contraintes de se livrer à des activités sexuelles devant une webcam par exemple.

Internet est également un excellent moyen pour les trafiquants de contrôler leurs victimes. Une pratique récurrente consiste à obtenir de la victime, lors de la phase de recrutement, des images sexuellement explicites et d'ensuite la menacer de distribuer les images si elle ne respecte pas les règles posées par le trafiquant. Ce type de chantage est connu sous le terme « *sextorsion* »⁸. Plus généralement les trafiquants peuvent communiquer en continu avec leurs victimes, leur donner des ordres et les menacer. L'utilisation d'Internet a par ailleurs l'avantage de permettre de surveiller une victime tout en étant séparé du lieu d'exploitation ; ce qui protège encore un peu plus les trafiquants.

⁶ C. DEMARÉE et C. VERHOFSTADT pour Child Focus, « Les victimes de proxénètes d'adolescents à Bruxelles - Étude exploratoire sur l'existence de la problématique et sa prise en charge possible à Bruxelles », juin 2020, p. 55, disponible sur https://childfocus.be/sites/default/files/child_focus-tienerpooiers-fr.pdf.

⁷ S. RAETS et J. JANSSENS, *op. cit.*, p.10.

⁸ *Ibid.*

Titre I. La traite sexuelle et Internet : incriminations et sanctions

Dans la première partie de ce travail nous entendons couvrir les comportements liés à l'utilisation d'Internet dans la traite sexuelle des personnes majeures ou mineures. Nous commençons par décrire l'infraction de traite des êtres humains en l'analysant d'un point de vue international, européen et enfin du point de vue du droit belge (Chapitre I). Nous nous intéressons ensuite plus spécifiquement à l'usage d'Internet pour recruter des personnes mineures en analysant les infractions de cyberprédation et de *grooming* (Chapitre II). Nous terminons par nous pencher sur l'usage d'Internet pour faire la publicité de services sexuels des victimes majeures comme mineures, et nous nous demandons dans quelle mesure la responsabilité des plateformes abritant du contenu relatif à des cas d'exploitation sexuelle peut être engagée (Chapitre III).

Chapitre I. La traite des êtres humains

Section I. Le Protocole de Palerme des Nations Unies

Le Protocole visant à prémunir, réprimer et punir la traite des personnes, en particulier des femmes et des enfants⁹ (ci-après « Protocole de Palerme ») est un texte additionnel à la Convention des Nations Unies contre la criminalité transnationale organisée¹⁰ (dite « Convention de Palerme »). Ces deux instruments complémentaires ont marqué le début de l'approche répressive du problème de la traite des êtres humains¹¹. La Convention de Palerme a pour objectif premier de promouvoir la coopération afin de prévenir et de combattre plus efficacement la criminalité transnationale organisée¹². Elle prévoit notamment l'incrimination de certains actes et des méthodes de coopération internationale entre les États parties¹³. La

⁹ Protocole additionnel à la Convention des Nations Unies contre la criminalité transnationale organisée visant à prévenir, réprimer et punir la traite des personnes, en particulier des femmes et des enfants, fait à New York le 15 novembre 2000, signé à Palerme le 12 décembre 2002, approuvé par la loi du 24 juin 2004, *M.B.*, 13 octobre 2004, p.71306 (ci-après « Protocole de Palerme »).

¹⁰ Convention des Nations Unies contre la criminalité transnationale organisée faite à New York 15 novembre 2000, signée à Palerme le 12 décembre 2002, approuvée par la loi du 24 juin 2004, *M.B.*, 13 octobre 2004, p.71306 (ci-après « Convention de Palerme »).

¹¹ O. NEDERLANDT, « Protection des victimes de traite des êtres humains – Approches internationales et européennes », *J.T.*, 2015/6, n° 6592, p. 158.

¹² Convention de Palerme, art. 1^{er}.

¹³ K. PLOUFFE-MALETTE, *Protection des victimes de traite des êtres humains*, Bruxelles, Bruylant, 2013, p. 39.

ratification de la Convention est obligatoire avant la ratification de quelconque Protocole additionnel¹⁴.

Le Protocole de Palerme est le premier instrument universel qui porte sur tous les aspects de la traite des êtres humains¹⁵. À ce jour, 178 États, dont la Belgique¹⁶ en sont parties. Le Protocole, qui s'interprète conjointement à la Convention, poursuit trois grands objectifs : prévenir et combattre la traite des personnes en accordant une attention particulière aux femmes et aux enfants, protéger et aider les victimes de la traite et promouvoir la coopération entre les États Parties¹⁷. C'est un instrument important en ce qu'il a réellement fait du traitement juridique et politique du problème de la traite des êtres humains une préoccupation mondiale¹⁸ et a grandement influencé d'autres normes adoptées ultérieurement au niveau du Conseil de l'Europe ou de l'Union européenne¹⁹.

Concernant le champ d'application du Protocole, celui-ci s'applique aux infractions de traite des êtres humains de nature transnationale et impliquant un groupe criminel organisé²⁰. Le Protocole, et la Convention à laquelle il se rapporte, souhaitent donc s'attaquer aux réseaux internationaux de traite. Les guides législatifs précisent toutefois que « l'élément transnational et l'implication d'un groupe criminel organisé ne doivent pas être considérés comme des éléments constitutifs de ces infractions aux fins d'incrimination »²¹.

En ratifiant le Protocole, les États parties se sont engagés à adopter les mesures législatives nécessaires afin de pénaliser les actes constitutifs de traite des êtres humains²². Le Protocole de

¹⁴ *Ibid.*, p.39 ; La Convention est complétée par trois Protocoles : Le Protocole relatif à la traite des personnes, le Protocole relatif au trafic illicite de migrants par terre, air et mer et le Protocole relatif à la fabrication et le trafic illicites d'armes à feu.

¹⁵ Protocole de Palerme, préambule.

¹⁶ Loi du 25 juin 2004 portant assentiment aux actes internationaux suivants : 1° la Convention des Nations unies contre la criminalité transnationale organisée; (...) ; 3° le Protocole additionnel la Convention des Nations unies contre la criminalité transnationale organisée visant à prévenir, réprimer et punir la traite des personnes, en particulier des femmes et des enfants, faits à New York le 15 novembre 2000; (...), *M.B.*, 13 octobre 2004, p. 701306.

¹⁷ Protocole de Palerme, art. 2.

¹⁸ K. PLOUFFE-MALETTE, *op.cit.*, p. 11.

¹⁹ C. CLESSE, « Les organisations internationales et la traite des êtres humains », in *Fondements et objectifs des incriminations et des peines en droit européen et international* (sous la dir. de D. BERNARD, Y. CARTUYVELS, C. GUILLAIN, D. SCALIA et M. VAN DE KERCHOVE), Limal, Anthemis, 2013, p.95.

²⁰ Protocole de Palerme, art. 4.

²¹ N. PASSAS et al., *Guides législatifs pour l'application de la Convention des Nations unies contre la criminalité transnationale organisée et des Protocoles s'y rapportant*, 1ere partie, New York, Publications des Nations Unies, 2004, p. 10.

²² Protocole de Palerme, art. 5 ; K. PLOUFFE-MALETTE, *op.cit.*, p. 46.

Palerme contient la première définition juridique internationale de la notion de « traite des personnes »²³ et ce afin d'assurer que les normes de droit interne soient suffisamment semblables pour permettre une coopération internationale efficace dans les enquêtes et les poursuites²⁴.

La traite y est définie comme « le recrutement, le transport, le transfert, l'hébergement ou l'accueil de personnes, par la menace de recours ou le recours à la force ou à d'autres formes de contrainte, par enlèvement, fraude, tromperie, abus d'autorité ou d'une situation de vulnérabilité, ou par l'offre ou l'acceptation de paiements ou d'avantages pour obtenir le consentement d'une personne ayant autorité sur une autre aux fins d'exploitation »²⁵. La définition de la traite donnée par le Protocole se compose donc de trois éléments : un acte, un moyen coercitif et les fins de l'exploitation²⁶.

L'acte - Concernant l'acte, il suffit que le présumé trafiquant ait agi avec comme but final l'exploitation de la victime pour qu'il y ait traite des êtres humains²⁷. La perpétration d'un acte caractéristique (recrutement, transport, transfert, etc.) avec l'intention d'exploiter une personne mais sans exploitation effective est suffisante²⁸.

Un moyen coercitif - L'acte constitutif doit avoir été réalisé à l'aide d'un moyen de coercition physique ou mental (menace, force, fraude, abus d'autorité)²⁹. Lorsqu'il y a eu emploi d'un des moyens visés dans la définition, le consentement de la victime à son exploitation est indifférent³⁰. En ce qui concerne la traite des enfants, la condition de l'usage d'un moyen de coercition disparaît³¹, de sorte que l'infraction est réalisée simplement par l'exécution d'un acte caractéristique (recrutement, hébergement, etc.) en vue d'exploiter un enfant. Le Protocole précise que le terme « enfant » désigne toute personne âgée de moins de 18 ans³².

²³ M.-A. BEERNAERT et P. LE COCQ, « La loi du 10 août 2005 modifiant diverses dispositions en vue de renforcer la lutte contre la traite et le trafic des êtres humains et contre les pratiques des marchands de sommeil. », *Rev. dr. pén.*, 2006/4, p. 338.

²⁴ N. PASSAS et al., *op.cit.*, p. 288.

²⁵ Protocole de Palerme, article 3 a).

²⁶ K. PLOUFFE-MALETTE, *op.cit.*, p. 47.

²⁷ *Ibid.*

²⁸ *Ibid.*

²⁹ K. PLOUFFE-MALETTE, *op. cit.*, p. 48.

³⁰ Protocole de Palerme, article 3 b).

³¹ Protocole de Palerme, article 3 c).

³² Protocole de Palerme, art. 3 d).

La finalité de l'exploitation – L'acte incriminé doit s'inscrire dans un objectif d'exploitation de la victime. Le terme exploitation doit comprendre au minimum « l'exploitation de la prostitution d'autrui ou d'autres formes d'exploitation sexuelle, le travail ou les services forcés, l'esclavage ou les pratiques analogues à l'esclavage, la servitude ou le prélèvement d'organes »³³. Le Protocole propose donc une liste non-exhaustive des formes de traite, le soin de définir plus précisément la notion d'exploitation étant confiée aux États parties³⁴. Ce standard minimum permet théoriquement de s'adapter à de nouvelles pratiques développées par les trafiquants, qui s'avèrent toujours plus inventifs lorsqu'il s'agit d'exploiter leurs victimes.

Au niveau de la peine, il faut noter que le Protocole de Palerme impose aux États parties de criminaliser la traite des êtres humains, mais ne prescrit pas de sanctions minimales.

Concernant l'aspect numérique, le Protocole ne traite pas particulièrement de la traite des enfants et des femmes par le biais de la technologie mais il est généralement admis que sa définition large englobe tout type de traite, même celle effectuée via Internet³⁵.

Section II. La Convention du Conseil de l'Europe sur la lutte contre la traite des êtres humains

La traite des êtres humains est une atteinte directe à l'objectif de défense des droits de la personne humaine qui se trouve au fondement même du Conseil de l'Europe³⁶. C'est pourquoi celui-ci a également adopté un instrument juridique visant à harmoniser les législations pénales nationales en matière de traite des êtres humains sous la forme d'une Convention³⁷.

La définition de traite des êtres humains retenue par la Convention du Conseil de l'Europe sur la lutte contre la traite des êtres humains³⁸ est la même que celle du Protocole de Palerme³⁹, si ce n'est que le Protocole utilise le terme « traite des personnes », et la Convention « traite des êtres humains »⁴⁰.

³³ Protocole de Palerme, art.3 a).

³⁴ C.-E. CLESSE, *La traite des êtres humains - Droit belge éclairé des législations française, luxembourgeoise et suisse*, Bruxelles, Larcier, 2013, p. 47.

³⁵ Y. KHALAILEH and N. KISSWANI, « Using technology in human trafficking: international law perspective and reflections within Middle Eastern countries », *Int. J. Technology Policy and Law*, 2015, Vol. 2, No. 1, p.39

³⁶ CONSEIL DE L'EUROPE, *Rapport explicatif de la Convention du Conseil de l'Europe sur la lutte contre la traite des êtres humains*, p.3, disponible sur <https://rm.coe.int/16800d388d>.

³⁷ Convention du Conseil de l'Europe sur la lutte contre la traite des êtres humains, signée à Varsovie le 16 mai 2005, approuvée par la loi du 3 juin 2007, *M.B.*, 27 juillet 2009, p.50141.

³⁸ Convention de Varsovie, art. 4.

³⁹ C. CLESSE, « Les organisations internationales et la traite des êtres humains », *op.cit.*, p.100.

⁴⁰ *Voy.* Convention de Varsovie, art. 4 et Protocole de Palerme, art. 3.

Le champ d'application de la Convention est plus large que celui du Protocole puisqu'elle vise toutes les formes de traite des êtres humains, qu'elles soient nationales ou transnationales et liées ou non à la criminalité organisée⁴¹.

Il est intéressant de noter que l'article 19 de la Convention demande aux parties d'envisager de conférer le caractère d'infraction pénale au fait d'utiliser, en connaissance de cause, les services d'une victime de traite des êtres humains. On décèle dans cette disposition la volonté de décourager la demande de services fournis par des personnes exploitées, une demande qui constitue un des facteurs qui favorisent la traite des êtres humains⁴². L'opportunité de l'adoption d'une telle mesure est toutefois laissée à l'appréciation des États et le rapport explicatif reconnaît les difficultés en matière de preuve que représente la condition de connaissance de l'exploitation par le client⁴³. Notons qu'en Belgique, il n'existe à ce jour aucune sanction pour l'achat de services sexuels d'une personne victime de traite⁴⁴.

La Convention oblige les États à prendre des mesures législatives pour condamner la complicité et la tentative se rapportant à l'incrimination de base⁴⁵. De la même manière, les États parties sont tenus d'adopter les dispositions législatives nécessaires afin que puissent être tenues responsables des personnes morales⁴⁶.

En ce qui concerne les sanctions, la Convention du Conseil de l'Europe « pallie à la faiblesse du protocole »⁴⁷ en exigeant des parties qu'elles adoptent des sanctions effectives, proportionnées et dissuasives⁴⁸ pour punir l'infraction de traite telle que décrite à l'article 4 de la Convention. Quatre circonstances aggravantes vont également être définies : la mise en danger de la vie de la victime délibérément ou par négligence grave, la minorité de la victime, le fait que l'infraction ait été commise par un agent public dans l'exercice de ses fonctions, le fait que l'infraction ait été commise dans le cadre d'une organisation criminelle⁴⁹.

⁴¹ Convention de Varsovie, art. 2.

⁴² I. ALGOET, « La traite des êtres humains : une nouvelle Hydre de Lerne ? Discours de rentrée prononcé à l'occasion de la rentrée de la cour du travail de Mons, le 4 septembre 2017 », *Rev. dr. pén. entr.*, 2018/1, p.14.

⁴³ CONSEIL DE L'EUROPE, *Rapport explicatif de la Convention du Conseil de l'Europe sur la lutte contre la traite des êtres humains*, *op.cit.*, p. 39.

⁴⁴ Sur ce sujet voy. L. LEVI, « Vers la pénalisation du client dans la lutte contre la prostitution forcée ? », *Rev. dr. pén.*, 2020/11, pp. 1021-1047.

⁴⁵ Convention de Varsovie, art. 21.

⁴⁶ Convention de Varsovie, art. 22.

⁴⁷ C. CLESSE, « Les organisations internationales et la traite des êtres humains », *op.cit.*, p.105.

⁴⁸ Convention de Varsovie, art. 23.

⁴⁹ Convention de Varsovie, art. 24.

Alors même qu'Internet jouait déjà un rôle important dans la mise en relation entre trafiquants, clients et victimes⁵⁰, la Convention n'en fait aucune mention⁵¹. Concernant la question de l'utilisation des nouvelles technologies de l'information en matière de traite des êtres humains, les rédacteurs de la Convention ont estimé que « la définition de la traite des êtres humains contenue dans la Convention trouve aussi à s'appliquer lorsque la traite est pratiquée via l'utilisation des nouvelles technologies de l'information. Ainsi, par exemple, lorsque la définition vise le recrutement d'une personne, ce recrutement est visé quelle que soit la manière dont il est effectué (que ce soit oralement, par voie de presse, via Internet, etc.). Il n'a donc pas été jugé nécessaire d'inclure une nouvelle disposition sur cette question dans la Convention pour que les dispositions de procédures et coopération internationale de la Convention sur la cybercriminalité [STE n°185] soient applicables à la traite des êtres humains »⁵².

Section III. La directive de l'Union européenne sur la traite des êtres humains

Trois instruments adoptés par l'Union européenne ont eu pour ambition de rapprocher les législations pénales matérielles en matière de traite des êtres humains⁵³. Le premier instrument contraignant adopté fut l'action commune du 24 février 1997 relative à la traite des êtres humains et à l'exploitation sexuelle des enfants⁵⁴. Ce texte fut remplacé par la décision-cadre relative à la lutte contre la traite des êtres humains⁵⁵. A son tour, cet instrument fut remplacé par une directive du 5 avril 2011⁵⁶.

La directive reprend la définition tripartite de l'infraction de traite des êtres humains⁵⁷ : une action, un moyen coercitif et la poursuite d'un objectif d'exploitation⁵⁸. Les actions comprises

⁵⁰ CONSEIL DE L'EUROPE, *Traite des êtres humains : recrutement par internet*, 2007, pp. 23-57, disponible sur <https://rm.coe.int/16806eeec1>.

⁵¹ S. TURGIS, « Chapitre 3. - Les droits de l'homme à l'heure d'Internet et du numérique : rupture ou continuité ? » in *L'Europe des droits de l'homme à l'heure d'Internet*, Bruxelles, Bruylant, 2019, p.94.

⁵² CONSEIL DE L'EUROPE, *Rapport explicatif de la Convention du Conseil de l'Europe sur la lutte contre la traite des êtres humains*, *op.cit.*, p.16.

⁵³ C. BRIÈRE et A. WEYEMBERGH, « L'Union européenne et la traite des êtres humains » in *Fondements et objectifs des incriminations et des peines en droit européen et international*, *op.cit.*, p.68.

⁵⁴ Action commune du 24 février 1997 adoptée par le Conseil sur la base de l'article K.3 du traité sur l'Union européenne, relative à la lutte contre la traite des êtres humains et l'exploitation sexuelle des enfants, *J.O.U.E.*, 4 mars 1997, L 63, p. 2.

⁵⁵ Décision-cadre 2002/629/JAI du Conseil du 19 juillet 2002 relative à la lutte contre la traite des êtres humains, *J.O.U.E.*, 1er août 2002, L 203, p. 1.

⁵⁶ Directive 2011/36/UE du Parlement européen et du Conseil du 5 avril 2011 concernant la prévention de la traite des êtres humains et la lutte contre ce phénomène ainsi que la protection des victimes et remplaçant la décision-cadre 2002/629/JAI du Conseil, *J.O.U.E.*, 15 avril 2011, L 101, p. 1 (ci-après « Directive traite »).

⁵⁷ Directive traite, art. 2.1.

⁵⁸ C. BRIÈRE et A. WEYEMBERGH, *op.cit.*, p. 77.

dans la définition sont le recrutement, le transfert, l'hébergement, l'accueil, et enfin la passation ou le transfert du contrôle exercé sur la victime. Cette dernière action ne figure pas dans la définition du Protocole des Nations Unies⁵⁹ qui sera reprise par le Conseil de l'Europe, en ce sens la définition donnée par la directive est plus large que les deux instruments précédents. Les finalités d'exploitation visées par le Protocole de Palerme et la Convention du Conseil de l'Europe se retrouvent dans la directive, qui ajoute par ailleurs dans la définition deux chefs d'exploitation : la mendicité et la criminalité forcée⁶⁰. Du reste, l'infraction de traite contenue dans la directive est similaire à celle du Protocole de Palerme.

Au niveau de la peine, la directive impose que l'infraction de traite soit punissable d'une peine privative de liberté, la peine maximale ne pouvant être inférieure à cinq ans⁶¹. En cas de circonstances aggravantes (liées à la vulnérabilité de la victime, l'existence d'une organisation criminelle, la mise en danger de la vie de la victime, le recours à des violences graves ou à un préjudice grave causé à la victime), la peine maximale ne peut être inférieure à dix ans⁶².

Section IV. Le droit belge : L'article 433quinquies du Code pénal

L'article 433quinquies, § 1er, 1°, de notre Code pénal punit le fait de recruter, de transporter, de transférer, d'héberger, d'accueillir une personne, de prendre ou de transférer le contrôle exercé sur elle et ce avec l'intention d'exploiter ou de contribuer à l'exploitation de cette personne dans l'une des fins légalement déterminées.

L'article 433quinquies vise différentes finalités d'exploitation. Ces finalités sont : l'exploitation sexuelle (1°), l'exploitation de la mendicité (2°), l'exploitation économique (3°), le prélèvement d'organes (4°) et la délinquance forcée (5°). Nous nous concentrons, dans le cadre de ce travail, sur la première forme de traite, à savoir l'exploitation de la prostitution ou toute autre forme d'exploitation sexuelle.

§1^{er}. Éléments constitutifs

L'incrimination de la traite contenue dans notre Code pénal est plus large que celle prévue par les instruments précités, car elle se caractérise par deux éléments constitutifs (actes et finalité

⁵⁹ *Ibid.* p. 78.

⁶⁰ *Ibid.*, pp.78-79.

⁶¹ Directive traite, art. 4.1.

⁶² Directive traite, art. 4.2.

de la traite) et non trois comme prévu dans les textes internationaux⁶³. La Belgique a en effet opté pour une extension de la définition en faisant basculer les moyens dans les circonstances aggravantes de l'infraction⁶⁴.

A. Élément matériel

1) Une action

L'infraction de traite des êtres humains est définie par le fait de poser certains actes typiques : recruter, transporter, transférer, héberger, accueillir, transférer ou prendre le contrôle d'une personne en vue d'exploiter cette personne⁶⁵.

L'énonciation de ces actions constitutives de traite, pourvu qu'elles soient posées dans un but particulier, permet des poursuites judiciaires à l'encontre de personnes agissant à différents stades du processus de traite des êtres humains⁶⁶. Ce n'est en effet pas forcément la même personne qui recrute, transporte, héberge la victime ou la met à disposition de l'exploitant. La disposition ainsi libellée répond à la nécessité de pouvoir incriminer chacun de ces comportements contribuant à l'exploitation de personnes⁶⁷. Notons que selon les modalités d'exécution de ces actes, ceux-ci peuvent constituer des infractions à d'autres dispositions du Code pénal⁶⁸.

À défaut de définition légale ou d'explications dans les travaux préparatoires, le terme « recrutement » doit être entendu dans son sens général⁶⁹, et peut être compris comme le fait « d'embaucher »⁷⁰. Il peut avoir lieu oralement, par voie de presse ou encore via Internet⁷¹. Le recrutement n'implique pas de mouvement transfrontalier, de sorte qu'un recrutement sur le territoire national est punissable⁷².

⁶³ J.-F. MINET, « L'évaluation de la politique belge en matière de lutte contre la traite des êtres humains : le rapport du GRETA », *Rev. dr. pén. entr.*, 2013/4, p. 106.

⁶⁴ C. CLESSE, « Les organisations internationales et la traite des êtres humains », *op.cit.*, p.100.

⁶⁵ F. KURZ, « Un trop long dimanche de fiançailles ou lorsque le respect de la tradition mène au viol et à la traite des êtres humains », *J.D.J.*, 2014/9, p. 26.

⁶⁶ C.-É. CLESSE, F. KURZ, P. LE COCQ et V. TRUILLET, *La traite des êtres humains et le travail forcé*, Bruxelles, Éditions Larcier, 2014, p. 19.

⁶⁷ *Ibid.*

⁶⁸ C.-E. CLESSE, « Chapitre XI - La traite des êtres humains » in *Les infractions – Volume 2 – Les infractions contre les personnes* (sous la coord. de H.D. BOSLY et C. DE VALKENNEER), Bruxelles, Larcier, 2020, p. 758.

⁶⁹ C.-E. CLESSE, « Le recrutement : une action active ou passive ? », note sous Cass., 8 octobre 2014, *Rev. dr. pén. crim.*, 2015, p.700.

⁷⁰ *Ibid.*, p.698.

⁷¹ *Ibid.*, p. 697

⁷² *Ibid.*, p. 698.

De la même manière que le recrutement n'implique pas de mouvement transfrontalier, le transport n'implique pas nécessairement le franchissement d'une frontière⁷³.

La loi du 29 avril 2013⁷⁴ a remplacé l'ancienne notion de « passation ou transfert de contrôle » qui figurait à l'article 433*quinquies* pour lui préférer l'expression « de prise ou de transfert de contrôle »⁷⁵. L'action de « prendre le contrôle » permet de prendre en compte une série de techniques utilisées par les exploitants pour exercer leur contrôle et leur influence sur leurs victimes⁷⁶. Parmi ces techniques, on peut citer l'adoption d'une attitude imposante, les hurlements, l'attachement amoureux, le mariage de complaisance, l'existence de dettes, la détermination d'horaires de travail, l'isolement ou encore la surveillance constante de la victime⁷⁷. Cet ascendant sur la victime doit ressortir des circonstances de fait⁷⁸.

Cette modification avait également comme but de couvrir de manière claire la vente et l'achat d'une personne en vue d'une exploitation⁷⁹. En effet, le fait de « vendre » une personne à un établissement ou à une personne à des fins d'exploitation est une action punissable en tant que telle et constitutive de traite des êtres humains, alors même qu'il n'y aurait pas encore eu de recrutement, de transport, d'accueil ou d'hébergement de la personne⁸⁰. Le terme vente ne figure par ailleurs pas expressément dans le texte de l'article 433*quinquies*, puisque, juridiquement parlant, une personne est hors commerce⁸¹.

2) Une personne

Toute personne peut être victime de traite des êtres humains à des fins d'exploitation sexuelle : femme ou homme, adulte ou mineur, et ce quelle que soit sa nationalité : belge, ressortissant de l'Union européenne ou ressortissant d'un pays tiers⁸². La régularité ou l'irrégularité de la présence de la victime sur le territoire belge est sans importance⁸³.

⁷³ CONSEIL DE L'EUROPE, *Rapport explicatif de la Convention du Conseil de l'Europe sur la lutte contre la traite des êtres humains*, *op.cit.*, p.16.

⁷⁴ Loi du 29 avril 2013 visant à modifier l'article 433 *quinquies* du Code pénal en vue de clarifier et d'étendre la définition de la traite des êtres humains, *M.B.*, 23 juillet 2013, p. 45880.

⁷⁵ A. DE NAUW et F. KUTY, *Manuel de droit pénal spécial*, Wolters Kluwer, 2018, pp. 512-513.

⁷⁶ *Ibid.*, p. 513.

⁷⁷ Projet de loi visant à modifier l'article 433*quinquies* du Code pénal afin d'étendre la définition de la traite des êtres humains à l'exploitation sexuelle, Rapport fait au nom de la Commission de la Justice, *Doc. parl.*, Ch. Repr., sess. ord. 2012- 2013, n° 53-2607/4, p. 8.

⁷⁸ C.-E. CLESSE, « Chapitre XI - La traite des êtres humains », *op.cit.*, p. 764.

⁷⁹ *Ibid.*

⁸⁰ Projet de loi modifiant diverses dispositions en vue de renforcer la lutte contre la traite et le trafic des êtres humains, Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord., 2004-2005, n° 1560/001, p. 18.

⁸¹ *Ibid.*

⁸² Circulaire du 23 décembre 2016 relative à la mise en œuvre d'une coopération multidisciplinaire concernant les victimes de la traite des êtres humains et/ou certaines formes aggravées de trafic des êtres humains, *M.B.*, 10 mars 2017, p. 35370.

⁸³ F. LAGASSE et M. PALUMBO, *Manuel de droit pénal social*, Bruxelles, Larcier, 2011, p. 244.

B. Élément moral

Pour tomber sous le coup de la définition de l'article 433*quinqies* du Code pénal, le comportement doit avoir été entrepris dans le but d'exploiter la personne en la soumettant à une des activités énoncées limitativement par la disposition. L'article 433*quinqies* 1° du Code pénal vise l'exploitation de la prostitution ou de toute autre forme d'exploitation sexuelle.

Au vu du caractère général des actes constituant l'élément matériel de l'infraction, l'élément moral joue un rôle important pour déterminer si on se trouve face à une infraction de traite des êtres humains. F. Kurz indique que : « l'infraction de traite des êtres humains doit toujours être examinée dans son intégrité complète : ce qui caractérise la traite des humains dans la législation belge, c'est le fait de poser des actes précis à des fins d'exploitation d'une personne, ce qui suppose que l'on soit très attentif à la question de l'intention criminelle. C'est la présence de cette intention spécifique qui rend le comportement de tel auteur punissable du chef de traite des êtres humains »⁸⁴.

L'infraction est donc subordonnée à une intention particulière, à savoir la finalité d'exploitation qui s'apparente alors à un dol spécial⁸⁵.

1) *Exploitation*

L'idée d'exploitation sous-tend généralement une recherche de bénéfice⁸⁶. Un des facteurs qui attire les exploitants sexuels est le caractère particulièrement lucratif de l'exploitation de la prostitution⁸⁷. La Cour de Cassation indique toutefois qu'il n'est pas requis par l'article 433*quinqies* du Code pénal que l'auteur des faits tire profit de l'exploitation⁸⁸.

⁸⁴ F. KURZ, *op.cit.*, p. 28.

⁸⁵ C. HUBERTS, « Les innovations de la loi du 10 août 2005 modifiant diverses dispositions en vue de renforcer la lutte contre la traite des êtres humains et le trafic des êtres humains et contre les pratiques des marchands de sommeil », *J.D.J.*, 2006, p.11.

⁸⁶ C.-E. CLESSE, *La traite des êtres humains - Droit belge éclairé des législations française, luxembourgeoise et suisse, op.cit.*, p. 317.

⁸⁷ Y.CHARPENEL, « L'exploitation de la prostitution, une affaire d'argent. », *Rev. dr. pén.*, 2013/9-10, p. 844.

⁸⁸ Cass., 5 juin 2018, *R.W.*, 2018-2019/9, p. 346.

2) *Exploitation seulement envisagée ou réalisée*

L'exploitation ne doit pas être réalisée pour que l'infraction soit consommée⁸⁹. Elle peut avoir simplement été envisagée lorsqu'une des actions visées par la définition a été accomplie⁹⁰. Ce sont les circonstances de l'espèce qui permettent aux cours et tribunaux d'établir l'existence de cet élément⁹¹. En conséquence, la traite des êtres humains existe préalablement à l'exploitation de la victime⁹². Les travaux préparatoires indiquent par exemple que : « *l'hébergement de jeunes filles entrées illégalement sur le territoire belge dans une maison appartenant à un proxénète notoire peut, selon les circonstances, laisser à penser qu'elles étaient destinées à la prostitution dans les vitrines qu'il contrôle* »⁹³.

En ce que la réalisation de l'infraction de traite ne nécessite pas une exploitation effective de la victime, l'article 433quinquies s'aligne sur les dispositions relatives au *grooming* et à la cyberprédation que nous analysons au chapitre II de ce travail. Ceci implique que pourrait être poursuivi un auteur qui aurait simplement recruté une victime mais qui ne l'aurait pas encore exploitée, si la traite des êtres humains a été découverte avant la finalisation du projet criminel consistant à exploiter la victime à des fins de prostitution par exemple⁹⁴.

3) *Exploitation de la prostitution ou toute autre forme d'exploitation sexuelle*

L'infraction de traite des êtres humains à des fins d'exploitation sexuelle est intrinsèquement liée à la prostitution, terme non-défini par la loi⁹⁵ mais par la jurisprudence comme désignant la personne qui moyennant rémunération se livre à des attouchements impudiques avec quiconque⁹⁶. Depuis la ratification de la Convention de New York de 1949⁹⁷, la Belgique a

⁸⁹ C.-E. CLESSE, *La traite des êtres humains - Droit belge éclairé des législations française, luxembourgeoise et suisse*, *op.cit.*, p. 317.

⁹⁰ A. DE NAUW et F. KUTY, *op.cit.*, p. 518.

⁹¹ D. CHICHOYAN, « Traite des êtres humains » in *Droit pénal et procédure pénale*, Malines, Wolters Kluwer, 2014, p.110.

⁹² CONSEIL DE L'EUROPE, *Rapport explicatif de la Convention du Conseil de l'Europe sur la lutte contre la traite des êtres humains*, *op.cit.*, p.17.

⁹³ Projet de loi modifiant diverses dispositions en vue de renforcer la lutte contre la traite et le trafic des êtres humains, Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2004-2005, n° 1560/001, p. 20.

⁹⁴ C.-E. CLESSE, « Chapitre XI - La traite des êtres humains », *op.cit.*, p. 766.

⁹⁵ A. MASSET, « Regard actualisé d'un pénaliste sur la prostitution », *R.F.D.L.*, 2015/1, p. 83.

⁹⁶ Cass., 3 janvier 1962, *Pas.*, 1962, I, p. 514.

⁹⁷ Convention des Nations Unies pour la répression de la traite des êtres humains et de l'exploitation de la prostitution d'autrui, approuvée par l'Assemblée générale dans sa résolution 317 (IV) du 2 décembre 1949, approuvée par la loi du 6 mai 1965, *M.B.*, 13 août 1965, p.9581.

intégré le cercle des pays abolitionnistes en matière de prostitution⁹⁸. Au moment de cette ratification en 1965, la Belgique avait en fait déjà abandonné l'approche réglementariste de la prostitution par l'adoption de la loi du 21 août 1948⁹⁹. Il en résulte qu'en Belgique le fait de se prostituer n'est pas une infraction¹⁰⁰. La prostitution en elle-même n'est ni légalisée ni pénalisée, et ce pour les majeurs comme pour les mineurs¹⁰¹. Le Code pénal réprime toutefois certains comportements qui entourent la prostitution, notamment ceux qui ont pour but d'organiser la prostitution ou d'en tirer profit. L'article 379 du Code pénal érige en infraction la participation à la débauche ou à la prostitution d'un mineur. L'article 380 punit ceux qui, par différents moyens, contribuent à la débauche et à la prostitution de personnes majeures (§1^{er}) ou mineures (§4). Notons que dans un tel régime abolitionniste, la distinction entre victimes de traite des êtres humains aux fins d'exploitation sexuelle et les personnes se liant à la prostitution de manière volontaire est plus complexe¹⁰². Spécialement lorsque selon certains, les prostituées ne peuvent être que des victimes¹⁰³.

L'ancien article 433*quinquies*, § 1^{er}, alinéa 1^{er}, 1^o, se référait uniquement aux infractions prévues aux articles 379 (favoriser la débauche d'un mineur), 380, § 1^{er} et 4 (exploitation de la prostitution et de la débauche), et 383*bis*, § 1^{er} (fabrication de matériel pédopornographique) du Code pénal¹⁰⁴. Seule la traite pour ces formes précises d'exploitation sexuelle était alors incriminée.

La loi du 29 avril 2013 a considérablement élargi le champ d'application de l'article 433*quinquies* §1^{er}, alinéa 1^{er}, 1^o en supprimant tout renvoi à d'autres articles du Code pénal et en introduisant dans la disposition les termes « ou d'autres formes d'exploitation sexuelle ». La finalité n'est donc plus de commettre des infractions bien précises énumérées dans le Code

⁹⁸ S. ANDRÉ, « Ceci n'est pas de l'abolitionnisme. Le régime juridique de la prostitution : un surréalisme à la belge ? », *Rev. Dr. ULiège*, 2017/3, p. 474.

⁹⁹ Loi du 21 août 1948 supprimant la réglementation officielle de la prostitution, *M.B.*, 13 septembre 1948, p. 7352.

¹⁰⁰ A. MASSET, « Regard actualisé d'un pénaliste sur la prostitution », *op.cit.*, p. 86.

¹⁰¹ L'Union européenne indique à ce sujet que les pays où la prostitution est légale ou non réglementée semblent être privilégiés par les trafiquants, qui usent d'un environnement légal favorable pour exploiter leurs victimes ; COMMISSION EUROPÉENNE, Deuxième rapport sur les progrès réalisés dans la lutte contre la traite des êtres humains (2018) établi conformément à l'article 20 de la directive 2011/36/UE concernant la prévention de la traite des êtres humains et la lutte contre ce phénomène ainsi que la protection des victimes, 2018, p. 4, disponible sur : <https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52018DC0777&from=FR>.

¹⁰² C. NAGELS et A. LEMONNE, « Titre IX - Traiter la traite : quand la prostituée navigue dans les eaux troubles de la dignité humaine » in *Sexe et normes*, Bruxelles, Bruylant, 2012, p. 228.

¹⁰³ *Ibid.*, p. 229.

¹⁰⁴ C. HUBERTS et J.-F. MINET, « La loi du 29 avril 2013 visant à modifier l'article 433*quinquies* du code pénal en vue de clarifier et d'étendre la définition de la traite des êtres humains: analyse et mise en perspective. », *Rev. dr. pén.*, 2014/1, p. 21.

pénal, mais couvre tout ce que le juge considérera comme une forme d'exploitation sexuelle¹⁰⁵. Les enquêteurs et magistrats ne sont plus pour cette finalité d'exploitation, « cadencés par une définition étroite et limitée »¹⁰⁶. Peuvent alors tomber sous le coup de cette disposition l'exploitation de la prostitution mais aussi d'autres formes d'exploitation sexuelle telles que la pornographie, les spectacles à caractère sexuel, l'esclavage sexuel, le tourisme sexuel ou encore les shows sur internet¹⁰⁷.

Des interrogations ont été soulevées à propos de l'articulation entre l'article 433^{quinq} et l'article 380 du Code pénal, qui réprime différentes formes de proxénétisme¹⁰⁸. L'identité des termes utilisés¹⁰⁹ dans les deux dispositions a suscité des questionnements quant à la portée des deux articles¹¹⁰. En réalité, l'article 380 du Code pénal peut s'avérer utile là où l'un des comportements visés par l'article 433^{quinq} préalable à l'exploitation (recrutement, hébergement, transfert) fait défaut ou ne peut être prouvé¹¹¹. Selon les situations¹¹² un comportement peut tomber sous l'application de l'un ou l'autre article, ou des deux, dans ce dernier cas les règles relatives au concours d'infractions seront applicables¹¹³. À ce sujet certains auteurs sont d'avis qu'il serait plus cohérent d'intégrer les articles 379 et 380 du Code pénal dans les éléments constitutifs de l'incrimination de traite des êtres humains¹¹⁴.

4) *Consentement de la victime*

La question du poids à accorder au consentement de la victime à son exploitation est une question fondamentale¹¹⁵. Qu'en est-il d'une victime qui, par exemple, était informée du fait qu'elle devrait se prostituer afin de rembourser le voyage depuis son pays d'origine ? Le Rapport de la Convention du Conseil de l'Europe indique que : « *la question du consentement*

¹⁰⁵ F. KURZ, *op.cit.*, p. 27.

¹⁰⁶ *Ibid.*

¹⁰⁷ C.-E. CLESSE, « Chapitre XI - La traite des êtres humains », *op.cit.*, p. 767.

¹⁰⁸ Voy. SERVICE DE LA POLITIQUE CRIMINELLE, Rapport bisannuel du Gouvernement relatif à la lutte contre la traite des êtres humains 2007-2008, p. 18, disponible sur <http://www.dsb-spc.be/doc/pdf/RapportTEH2007-2008fr.pdf>.

¹⁰⁹ Les articles 380 §1^{er}, 4° et §4, 4° visent la personne qui aura embauché ou entraîné une personne en vue de la débauche ou de la prostitution. Les articles 380 §1^{er}, 4° et §4, 4° visent quiconque aura, de quelque manière que ce soit, exploité la débauche ou la prostitution d'autrui.

¹¹⁰ C. HUBERTS et J.-F. MINET, *op.cit.*, p. 23.

¹¹¹ *Ibid.*, p.24.

¹¹² Pour des exemples voy. *Ibid.* pp. 24-25.

¹¹³ C.pén., art. 65.

¹¹⁴ Voy. G. VERMEULEN, « Een stille seksuele strafrechtsrevolutie. Verrassende realiteitszin inzake seksueel strafrecht in het nieuwe Strafwetboek », *Panopticon*, 2018/6, p. 487.

¹¹⁵ C.-E. CLESSE, F. KURZ, P. LE COCQ et V. TRUILLET, *op.cit.*, p. 5.

*n'est pas si simple et il n'est pas aisé de déterminer où le libre choix s'arrête et où commence la contrainte. En matière de traite certaines personnes ne savent pas du tout ce qui les attend d'autres savent parfaitement qu'il s'agit, par exemple, de se prostituer. Cependant, même si une personne souhaite trouver un travail, et éventuellement se prostituer, cela ne signifie pas qu'elle consent à subir des abus de toutes sortes»*¹¹⁶.

L'article 433quinquies, §1^{er}, alinéa 2 précise que le consentement de la victime n'a pas d'importance, de sorte que ce consentement n'est pas de nature à ôter au comportement de l'exploitant son caractère illégal. L'auteur des faits ne peut invoquer un consentement donné à l'exploitation pour échapper à sa responsabilité pénale. La notion d'exploitation n'est donc pas incompatible avec le consentement de la victime¹¹⁷. Le droit belge entend par cela apporter une plus grande protection aux victimes, qui peuvent parfois consentir à leur exploitation en raison de la grande vulnérabilité dans laquelle elles se trouvent. Certaines jeunes filles, désireuses de fuir une vie précaire et sans perspectives, choisissent délibérément la voie de l'exploitation, qui leur semble être un prix à payer acceptable en contrepartie des avantages supposés qu'elles en tireront. Notons que, dans une même logique en matière d'exploitation sexuelle, l'article 380 du Code pénal indique que le consentement de la personne prostituée n'a pas d'importance.

C. Clarifications quant à la nécessité d'une filière

La loi du 29 avril 2013 avait également pour objectif de clarifier la nécessité de l'existence d'une filière criminelle pour que l'infraction de traite à finalité d'exploitation sexuelle soit retenue. L'ancienne formulation de l'article 433quinquies (« afin de permettre la commission de l'infraction... ») avait donné lieu à des interprétations divergentes sur l'étendue de l'incrimination de traite à des fins d'exploitation sexuelle¹¹⁸. En effet, certaines juridictions de fond ont adopté une interprétation restrictive de l'article 433quinquies §1^{er} alinéa 1^{er}, 1^o et ont rejeté cette qualification au motif de l'absence de filière criminelle¹¹⁹. Cette interprétation était problématique pour plusieurs raisons. Premièrement, elle allait à l'encontre des objectifs de la loi qui voulait que l'infraction de traite des êtres humains ne soit plus limitée aux seuls étrangers, l'exigence d'une filière avait pour effet de ne pas prendre en compte les victimes

¹¹⁶ CONSEIL DE L'EUROPE, *Rapport explicatif de la Convention du Conseil de l'Europe sur la lutte contre la traite des êtres humains*, op. cit., p. 18.

¹¹⁷ A. DE NAUW et F. KUTY, op.cit., p. 514.

¹¹⁸ C. HUBERTS et J.-F. MINET, op.cit., p. 9.

¹¹⁹ Voy. not. Corr. Liège (8^e ch.), 11 février 2009, *Rev.dr.pén.crim.*, p. 963.

belges recrutées et exploitées en Belgique, en ce que ces victimes ne passent généralement pas par une filière¹²⁰. Deuxièmement, elle avait pour effet de priver une catégorie de personnes exploitées de leur statut de victime¹²¹. Enfin cette interprétation créait une différence de traitement, très certainement injustifiée, entre les victimes d'exploitation sexuelle d'une part et les victimes d'une autre forme d'exploitation d'autre part¹²².

À propos de l'ancienne formulation qui avait donné lieu à des controverses, les travaux préparatoires de la loi du 29 avril 2013 indiquent que : « *ce libellé a semé la confusion et a conduit certaines juridictions à adopter une interprétation erronée de la disposition, en subordonnant son application à l'existence d'une filière, lorsque la finalité visait le seul verbe "permettre". Le présent amendement vise à reformuler l'infraction en utilisant l'expression "à des fins de"* »¹²³. Il ne fait donc aujourd'hui plus de doute que l'existence d'un réseau criminel n'est pas exigée pour retenir la qualification de traite des êtres humains à des fins d'exploitation sexuelle, comme à d'autres fins d'exploitation.

§2. La peine

L'infraction de traite des êtres humains est punie d'un emprisonnement d'un an à cinq ans et d'une amende de cinq cents euros à cinquante mille euros¹²⁴. Les amendes pouvant être prononcées doivent être multipliées par le nombre de victimes d'exploitation¹²⁵. La tentative est punie d'un emprisonnement d'un à trois ans et d'une amende de cent euros à dix mille euros¹²⁶.

Les articles 433sexies, 433septies et 433octies du Code pénal organisent trois niveaux¹²⁷ de circonstances aggravantes¹²⁸.

¹²⁰ D. DESAIVE, « La coexistence des préventions visées aux articles 433quinquies, § 1, 1°, et 380, alinéa 1, 1° et 4°, du Code pénal », *Rev. dr. pén.*, 2010, liv. 7-8, p. 970.

¹²¹ *Ibid.*

¹²² *Ibid.*, p. 971.

¹²³ Projet de loi visant à modifier l'article 433quinquies du Code pénal afin d'étendre la définition de la traite des êtres humains à l'exploitation sexuelle, Amendement n° 1 de Mme Van Cauter, *Doc. parl.*, Ch. repr., sess. ord. 2012-2013, n° 53-2607/2, p. 2.

¹²⁴ C. pén., art. 433quinquies, §2.

¹²⁵ C.pén., art. 433quinquies, §4.

¹²⁶ C.pén., art. 433quinquies, §3.

¹²⁷ Projet de loi modifiant diverses dispositions en vue de renforcer la lutte contre la traite et le trafic des êtres humains, Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2004-2005, n° 1560/001, p. 12.

¹²⁸ T. HENRION, « Protection pénale des mineurs » in *Droit pénal et procédure pénale*, Malines, Wolters Kluwer, 2017, p.117.

Le premier niveau de circonstances aggravantes de l'article 433^{sexies} tient à la qualité de l'auteur de l'infraction. La disposition vise les hypothèses où l'infraction a été commise par une personne qui a autorité sur la victime ou qui a abusé de l'autorité ou des facilités que lui confèrent ses fonctions (1°) ou par un officier ou fonctionnaire public, un dépositaire ou agent de la force publique agissant à l'occasion de l'exercice de ses fonctions (2°).

Le deuxième niveau de circonstances aggravantes, visées à l'article 433^{septies}, a trait au *modus operandi* de l'infraction. Comme nous l'avons déjà mentionné, le législateur n'a pas repris les moyens en tant qu'éléments constitutifs de l'infraction mais a fait le choix d'en faire des circonstances aggravantes¹²⁹. La traite des êtres humains est alors centrée autour du concept de l'exploitation, et non sur les moyens qui ont mené à cette exploitation¹³⁰.

L'article 433^{septies} prévoit une aggravation de la peine lorsque l'infraction a été commise envers un mineur (1°), lorsqu'elle a été commise en abusant de la situation de vulnérabilité d'une personne (2°), lorsqu'elle a été commise en faisant usage de manœuvres frauduleuses, de violence, de menaces ou de quelque forme de contrainte (3°), lorsqu'elle a été commise au moyen de l'offre ou de l'acceptation de paiements ou d'avantages quelconques pour obtenir le consentement d'une personne ayant autorité sur la victime (3bis°), lorsque la vie de la victime a été mise en danger délibérément ou par négligence grave (4°), lorsque l'infraction a causé une maladie paraissant incurable, une incapacité de travail personnel de plus de quatre mois, la perte complète d'un organe ou de l'usage d'un organe ou une mutilation grave (5°), lorsque l'activité concernée constitue une activité habituelle (6°) ou enfin lorsque l'activité constitue un acte de participation à l'activité principale ou accessoire d'une association au sens de l'article 322 du Code pénal¹³¹ (7°).

Le troisième niveau de circonstances aggravantes est prévu par l'article 433^{octies}. La peine est aggravée lorsque l'infraction a causé la mort de la victime sans intention de la donner (1°) ou lorsqu'elle constitue un acte de participation à l'activité principale ou accessoire d'une organisation criminelle au sens de l'article 324bis du Code pénal¹³² (2°).

¹²⁹ C. HUBERTS, *op.cit.*, pp. 10-11.

¹³⁰ C. HUBERTS et J.-F. MINET, *op.cit.*, p. 14.

¹³¹ L'article 322 du Code pénal indique que toute association formée dans le but d'attenter aux personnes ou aux propriétés est un crime ou un délit, qui existe par le seul fait de l'organisation de la bande.

¹³² L'article 324bis du Code pénal indique que Constitue une organisation criminelle l'association structurée de plus de deux personnes, établie dans le temps, en vue de commettre de façon concertée, des crimes et délits punissables d'un emprisonnement de trois ans ou d'une peine plus grave, pour obtenir, directement ou indirectement, des avantages patrimoniaux.

Une loi récente¹³³ a consacré le principe de non-sanction des victimes de traite et ce quel que soit le type d'exploitation subi. Le Code pénal prévoit désormais que la victime de traite des êtres humains qui prend part à des infractions en conséquence directe de son exploitation, n'encourt aucune peine du chef de ces infractions. Ce principe de non-sanction, qui prend la forme d'une cause d'excuse absolutoire, est un élément essentiel de la lutte contre la traite des êtres humains, car les victimes sont parfois forcées de commettre des infractions contre leur gré. Les travaux parlementaires indiquent que l'objectif de la clause de non-sanction est triple¹³⁴. Il s'agit en premier lieu de préserver les droits humains des victimes privées de leur libre arbitre. Ensuite, cela permet d'éviter aux victimes des sanctions injustes et d'adopter une approche judiciaire cohérente, tout en permettant de prévenir de nouvelles victimisations. Enfin, la non-sanction permet d'inciter les victimes à porter plainte contre les auteurs et à intervenir comme témoins. Actuellement, rares sont les victimes qui osent parler par crainte d'être sanctionnées pour des infractions qu'elles auraient elles-mêmes commises. Or les travaux parlementaires soulignent le caractère déterminant de la collaboration des victimes pour condamner les auteurs de traite¹³⁵.

Chapitre II. La cyberprédation et le *grooming*

Le recours grandissant à Internet et aux réseaux sociaux pour recruter des victimes signifie que les enfants et adolescents sont particulièrement exposés. Ces derniers sont considérés comme des personnes plus vulnérables dans le cyberspace, et doivent bénéficier à ce titre de protections particulières¹³⁶. Bien qu'Internet fasse partie du quotidien de ces « natifs du numérique », le monde virtuel les expose au risque de rencontrer des prédateurs, particulièrement dans le domaine sexuel¹³⁷.

L'article 23 de la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels¹³⁸ (Convention de Lanzarote), adoptée le 25 octobre 2007,

¹³³ Loi du 22 mai 2019 relative au trafic d'organes humains et relative au principe de non-sanction des victimes de traite des êtres humains, *M.B.*, 21 juin 2019, p. 63970.

¹³⁴ Proposition de loi incriminant le commerce d'organes et le tourisme de transplantation, Rapport fait au nom de la commission de la santé publique, de l'environnement et du renouvellement de la société, *Doc. parl.*, Ch. repr., sess. ord. 2018-2019, n° 54-3537/004, pp.5-6.

¹³⁵ *Ibid.*, p.6.

¹³⁶ G. MATHIEU et A.-C. RASSON, « Chapitre 11 - Les droits de l'enfant dans l'environnement numérique : à la recherche d'un subtil équilibre entre protection et autonomie » in *Vulnérabilités et droits dans l'environnement numérique*, Bruxelles, Larcier, 2018, p. 398.

¹³⁷ A. MASSET, « Protection des mineurs en ligne en droit pénal belge » in *Société numérique et droit pénal Belgique, France, Europe* (sous la dir. de V. FRANSEN et D. FLORE), Bruxelles, Bruylant, 2019, p. 67.

¹³⁸ Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels, signée à Lanzarote le 25 octobre 2007, approuvée par la loi du 7 février 2012, *M.B.*, 21 juin 2013, p. 39977.

imposait aux États membres d'ériger en infraction pénale la sollicitation en ligne d'enfants à des fins sexuelles (*online grooming*). De la même manière, l'article 6 de la directive 2011/93/UE¹³⁹ du Parlement européen et du Conseil du 13 décembre 2011 appelait les États membres à prendre les mesures nécessaires pour que soit punissable la sollicitation en ligne d'enfants à des fins sexuelles. À l'époque, le droit pénal belge ne possédait pas de législation spécifique pour poursuivre ce type de comportements¹⁴⁰.

C'est ainsi que, le 10 avril 2014, deux lois¹⁴¹ ont été promulguées pour moderniser le Code pénal, notamment en ce qui concerne les infractions commises contre les mineurs via Internet ou d'autres technologies de la communication. La première loi a inséré dans le Code pénal un nouvel article 433*bis*/1 en vue de protéger les enfants contre les cyber-prédateurs. La deuxième loi cherche plus spécifiquement à lutter contre le phénomène du *grooming* en ligne. Ces introductions dans le Code pénal s'avéraient nécessaires en premier lieu dans le domaine de la délinquance sexuelle¹⁴². Cette adaptation s'est faite en réponse au constat inquiétant que les mineurs, enfants et adolescents, étaient et sont encore de plus en plus souvent approchés et abusés via Internet, où l'auteur jouit d'un anonymat sans précédent qui lui permet de mentir sur son identité et ses caractéristiques personnelles, telles que son âge¹⁴³. Le législateur a alors voulu criminaliser ces actes préparatoires de manière indépendante, avant même tout abus sur la personne du mineur¹⁴⁴ et permettre l'identification et l'interpellation des auteurs avant tout passage à l'acte¹⁴⁵.

Un même comportement, à savoir le recrutement de personnes mineures en ligne en vue de les exploiter sexuellement peut être à la fois constitutif de traite (433*quinquies* C. pén.) d'une part, et de grooming (377*quater* C.pén.) ou de cyberprédation (433*bis*/1 C.pén) d'autre part¹⁴⁶.

¹³⁹ Directive 2011/92/UE du Parlement européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI du Conseil, *J.O.U.E.*, 17 décembre 2011, L 335, p.1.

¹⁴⁰ On pouvait considérer qu'il s'agissait d'une tentative de corruption de la jeunesse (379 C.pén.) ; M. GIACOMETTI et P. MONVILLE, « 6 - Réseaux sociaux, anonymat et faux profils : vrais problèmes en droit pénal et de la procédure pénale » in *Les réseaux sociaux et le droit*, Bruxelles, Larcier, 2014, p. 189.

¹⁴¹ Loi du 10 avril 2014 relative à la protection des mineurs contre la sollicitation à des fins de perpétration d'infractions à caractère sexuel, *M.B.*, 30 avril 2014, p. 35484 ; Loi du 10 avril 2014 modifiant le Code pénal en vue de protéger les enfants contre les cyberprédateurs, *M.B.*, 30 avril 2014, p. 35486.

¹⁴² L. STEVENS, « Grooming en cyberlokkig strafbaar. Uitbreiding van de strafrechtelijke bescherming van de seksuele integriteit van minderjarigen in cyberspace », *R.W.*, 2014-2015/22, p. 844.

¹⁴³ A. DIERICKX, « Noot nieuwe seksuele criminaliteit tot nieuwe seksuele misdrijven ? », *N.C.*, 2017/3, p. 220-221.

¹⁴⁴ A. MASSET, « Protection des mineurs en ligne en droit pénal belge », *op.cit.*, p.67.

¹⁴⁵ *Ibid.*

¹⁴⁶ Corr. Gand, 28 juin 2018, disponible sur : https://www.myria.be/files/h18-06-29_corr_Gent.pdf.

Section I. La cyberprédation

i) Définition

La prédation sur internet vise de manière générale « tout comportement d'un majeur tendant à entrer en contact avec un mineur dans le but, par la suite, d'échanger avec ce dernier, ces échanges étant de nature à conduire à la commission d'infractions sur la personne du mineur »¹⁴⁷.

ii) Éléments constitutifs

L'article 433*bis*/1 du Code pénal pénalise le comportement du cyber-prédateur, c'est-à-dire la personne majeure qui communique par le biais des technologies de l'information et de la communication avec un mineur avéré ou supposé, et ce en vue de faciliter la perpétration à son égard d'un crime ou d'un délit, s'il a dissimulé ou menti sur son identité ou son âge ou sa qualité, s'il a insisté sur la discrétion à observer quant à leurs échanges, s'il a offert ou fait miroiter un cadeau ou un avantage quelconque ou s'il a usé de toute autre manœuvre.

Sont protégés par cette disposition les mineurs de moins de 18 ans. Plus encore, la loi entend punir les manœuvres réalisées à l'égard d'un mineur mais également à l'égard des personnes majeures que l'auteur pensait mineures, ainsi qu'il ressort des termes « mineur avéré ou supposé » dans l'article 433*bis*/1 du Code pénal. Ce qui doit être considéré n'est donc pas seulement l'âge réel de la victime mais l'âge que celle-ci avait selon l'auteur lorsqu'il a échangé avec elle¹⁴⁸. Ce prolongement de l'incrimination aux communications à l'égard des personnes que l'auteur pensait mineures suscite des critiques quant au principe de légalité¹⁴⁹. En effet, il peut être délicat d'apporter la preuve de ce que l'auteur avait la conviction que la victime était mineure¹⁵⁰.

L'élément matériel vise plusieurs communications entre la personne majeure et le mineur. Ces actes doivent s'étaler sur une certaine période de temps et être destinés à abuser de la faiblesse du mineur¹⁵¹. Ce qui est visé par la disposition c'est une véritable stratégie de manipulation de

¹⁴⁷ J.-F. HENROTTE et F. JONGEN, *Pas de droit sans technologie*, Bruxelles, Larcier, 2015, p. 226.

¹⁴⁸ J.-F. HENROTTE et F. JONGEN, *op.cit.*, p. 245.

¹⁴⁹ *Ibid.*

¹⁵⁰ *Ibid.*

¹⁵¹ Proposition de loi modifiant le Code pénal en vue de protéger les enfants contre les cyberprédateurs, Rapport fait au nom de la commission de la justice, *Doc. Parl.*, Ch. repr., sess. ord. 2013-2014, n° 53-3450/002, p.4.

la part de la personne majeure, de sorte qu'un seul message ne suffirait pas¹⁵². Il n'est pas nécessaire qu'une rencontre ait effectivement eu lieu ou ait même été proposée pour que le comportement tombe sous le coup de l'article 433bis/1¹⁵³. De plus, il n'est pas nécessaire que l'initiative de la communication soit le fait du majeur, le premier contact peut avoir été pris par le mineur¹⁵⁴. Les communications sanctionnées sont celles qui se déroulent au moyen des technologies de l'information et de la communication. Ceci comprend Internet et plus largement tout mode de communication électronique : réseaux sociaux, applications de communication (Skype, WhatsApp, Viber), forums, et autres.

La personne majeure entrant en contact avec le mineur ne doit pas avoir eu l'intention de commettre sur le mineur une infraction à caractère sexuel¹⁵⁵. En effet, les infractions contre l'intégrité sexuelle ne sont pas les seules visées, la disposition vise plus généralement le leurre de mineurs à des fins délictuelles ou criminelles. En ce sens, cette infraction dépasse la portée des obligations contenues dans la Convention de Lanzarote et la Directive de l'Union européenne¹⁵⁶. L'élément moral consiste donc en un dol spécial, à savoir l'intention d'entrer en contact avec un mineur afin de faciliter la commission d'une infraction à son détriment¹⁵⁷. En pratique, les infractions comme celle-ci qui reposent en grande partie sur une intention spéciale peuvent s'avérer difficiles à prouver. De ce fait, cette disposition trouvera probablement à s'appliquer à un stade où il ressort clairement que les échanges étaient destinés à commettre une infraction sur la personne du mineur¹⁵⁸. En matière de traite sexuelle, cela signifie que, dans la plupart des cas, ces comportements ne seront probablement pas punis avant que la victime ait été exploitée.

iii) La peine

La cyberprédation est punie par un emprisonnement allant de trois mois à cinq ans. La tentative de ce délit n'est pas punissable.

¹⁵² A. MASSET, « Protection des mineurs en ligne en droit pénal belge », *op.cit.*, p. 71.

¹⁵³ J.-F. HENROTTE et F. JONGEN, *op.cit.*, p. 242.

¹⁵⁴ *Ibid.*

¹⁵⁵ *Ibid.*

¹⁵⁶ A. MASSET, « Protection des mineurs en ligne en droit pénal belge », *op.cit.*, p. 72.

¹⁵⁷ J.-F. HENROTTE et F. JONGEN, *op.cit.*, p. 246.

¹⁵⁸ *Ibid.*

Section II. La sollicitation de mineurs à des fins sexuelles

i) L'article 377^{quater} du Code pénal

L'article 377^{quater} du Code pénal a été intégré par la loi du 10 avril 2014 relative à la protection des mineurs contre la sollicitation à des fins de perpétration d'infractions à caractère sexuel dans le Chapitre V du Code pénal « *Du voyeurisme, de la diffusion non consensuelle d'images et d'enregistrements à caractère sexuel, de l'attentat à la pudeur et du viol* ». Celui-ci punit la personne majeure qui, par le biais des technologies de l'information et de la communication, propose une rencontre à un mineur de moins de seize ans accomplis dans l'intention de commettre une des infractions visées aux chapitres V, VI (« *De la corruption de la jeunesse et de la prostitution* ») et VII (« *Des outrages public aux bonnes mœurs* ») du Titre VI du Code pénal. Ces chapitres contiennent les infractions relatives à l'incitation à la débauche de mineurs (art. 379 C.pén.), aux différentes formes de proxénétisme (art. 380 C.pén.) et à la pédopornographie (art. 383^{bis} C.pén.).

L'utilisation du terme « *grooming* » n'appartenait pas au langage courant lors de l'introduction de la loi, de sorte que le législateur a fait le choix de ne pas l'inclure dans la description de l'infraction, mais de faire correspondre le nouvel article 377^{quater} du Code pénal aux définitions figurant dans la Convention de Lanzarote et dans la Directive 2011/99/UE¹⁵⁹.

ii) Définition du *grooming*

Le terme anglophone « *grooming* » peut se traduire comme « prendre soin, préparer » et est employé pour désigner la pratique qui consiste à approcher l'enfant ou l'adolescent et établir une relation de confiance dans le but d'abaisser ou d'éliminer progressivement les barrières du mineur afin de le préparer à des abus sexuels¹⁶⁰. Cette infraction est plus ciblée que celle de la cyberprédation, car elle concerne uniquement la sollicitation de mineurs à des fins sexuelles. Dans ce contexte, l'abus sexuel n'est pas le résultat d'une série de facteurs aléatoires, mais bien l'aboutissement d'un processus délibéré et bien organisé¹⁶¹. Certains qualifient à cet égard la pratique du *grooming* comme « l'antichambre de l'abus sexuel »¹⁶².

Le *grooming* n'est pas un phénomène nouveau, l'utilisation du terme anglophone pour décrire la problématique est par ailleurs relativement récente. La sollicitation hors ligne, dans la vie réelle, d'enfants à des fins sexuelles (*offline grooming*) est une stratégie d'abus très ancienne,

¹⁵⁹ A. DIERICKX, *op.cit.*, p. 219.

¹⁶⁰ L. STEVENS, *op.cit.*, p. 847.

¹⁶¹ *Ibid.*

¹⁶² A. MASSET, « Protection des mineurs en ligne en droit pénal belge », *op.cit.*, p. 68.

tandis que leur sollicitation en ligne (*online grooming*) est un phénomène plus récent¹⁶³, apparu avec le développement des nouvelles technologies de l'information¹⁶⁴.

iii) Éléments constitutifs

Le *grooming* en ligne n'est un délit que si le comportement est commis par un adulte qui s'adresse à un enfant de moins de seize ans¹⁶⁵. L'infraction ne peut être commise que par une personne âgée de dix-huit ans ou plus sur une victime âgée de moins de seize ans, c'est-à-dire les jeunes qui n'ont pas encore atteint la majorité sexuelle¹⁶⁶. La disposition ne protège donc pas les mineurs de plus de 16 ans. Comme l'explique L. Stevens¹⁶⁷, la disposition est limitée aux mineurs n'ayant pas atteint la majorité sexuelle¹⁶⁸, dans la mesure où le développement relationnel et sexuel des jeunes à l'heure actuelle se fait aussi via Internet, qui représente pour eux un élément naturel de leur quotidien et un outil indispensable de communication.

La proposition de rencontre physique constitue l'élément principal de l'infraction¹⁶⁹. Pour que l'article 377*quater* soit applicable, l'auteur doit avoir proposé une rencontre au mineur¹⁷⁰. L'échange de messages ou d'images à caractère sexuel sans proposition de rencontre ne constitue pas en soi une infraction et échappe à la définition du *grooming online*¹⁷¹. De tels comportements sont potentiellement répréhensibles sur base d'autres dispositions du Code pénal, telle que la détention de matériel pédopornographique¹⁷² ou la cyberprédation¹⁷³. En outre, la proposition de rencontre doit avoir été suivie d'actes matériels visant à réaliser la dite rencontre, dans le monde physique. De vagues intentions, sans éléments concrets ne sauraient suffire. Par contre, la condition sera remplie si l'auteur a préparé la rencontre, par exemple en planifiant un itinéraire, en achetant des billets de train, en prenant congé au travail, ou en se présentant au lieu de rendez-vous¹⁷⁴. Il appartient au juge du fond d'apprécier la suffisance des

¹⁶³ Proposition de loi modifiant le Code pénal en vue de garantir la protection pénale des enfants contre le « grooming » (mise en confiance à des fins d'abus sexuel), Développements, *Doc. parl.*, Sén., sess. ord. 2012-2013, n° 5-1823/1, p. 2.

¹⁶⁴ G. MATHIEU, « Chapitre 16. - Les droits de l'enfant et Internet : entre autonomie et protection » in *L'Europe des droits de l'homme à l'heure d'Internet*, *op.cit.*, p. 608.

¹⁶⁵ L. STEVENS, *op.cit.*, p. 848.

¹⁶⁶ *Ibid.*

¹⁶⁷ *Ibid.*

¹⁶⁸ En Belgique, l'âge de la majorité sexuelle est actuellement fixé à 16 ans par l'article 372 du Code pénal qui stipule : « Tout attentat à la pudeur commis sans violences ni menaces sur la personne ou à l'aide de la personne d'un enfant de l'un ou de l'autre sexe, âgé de moins de seize ans accomplis, sera puni de la réclusion de cinq ans à dix ans ». A partir de 16 ans, un mineur peut avoir légalement des relations sexuelles et est présumé y consentir.

¹⁶⁹ J.-F. HENROTTE et F. JONGEN, *op.cit.*, p.232.

¹⁷⁰ A. MASSET, « Protection des mineurs en ligne en droit pénal belge », *op.cit.*, p. 69.

¹⁷¹ *Ibid.*

¹⁷² C. pén., art. 383*bis*.

¹⁷³ L. STEVENS, *op. cit.*, p. 849.

¹⁷⁴ *Ibid.*

moyens mis en œuvre par l’auteur attestant de sa volonté que la rencontre ait lieu¹⁷⁵. En revanche, la condition est indiscutablement remplie si la rencontre a effectivement eu lieu¹⁷⁶.

Les travaux parlementaires précisent toutefois qu’il n’est pas nécessaire que le contact sur Internet mène effectivement à un contact physique entre l’auteur et l’enfant, ni même que l’enfant se soit livré à une activité sexuelle¹⁷⁷. Si rencontre il y a, la loi n’exige pas qu’une infraction visée aux articles 372 à 389 du Code pénal ait été effectivement commise sur la personne du mineur de moins de seize ans¹⁷⁸. Conformément à la Convention de Lanzarote et à la directive européenne, l’article 377^{quater} met véritablement l’accent sur la phase de communication et de manipulation, durant laquelle l’auteur gagne la confiance du mineur¹⁷⁹.

L’utilisation des technologies de l’information ou de la communication est une condition *sine qua non* de l’application de la sanction pénale. Comme pour la cyberprédation, le terme est relativement large et comprend notamment les moyens suivants : Internet, forums de discussion, réseaux sociaux, courriels, SMS, MMS, chats, webcam ou encore messageries instantanées.

L’élément moral correspond à un dol spécial à caractère sexuel¹⁸⁰. La proposition de rencontre de la part de l’auteur doit avoir été motivée par une intention spécifique, à savoir celle de commettre un abus physique sur le mineur¹⁸¹. La preuve de cet élément peut poser des difficultés. Le plus souvent celle-ci sera rapportée par l’examen des communications électroniques échangées avec le mineur sur un système informatique appartenant au suspect¹⁸².

iv) La peine

Le *grooming* est puni d’une peine d’emprisonnement d’un à cinq ans¹⁸³. La tentative n’est pas punissable.

¹⁷⁵ O. LEROUX, « Section 2. - Criminalité informatique aspécifique » in *Les infractions – Volume 1*, Bruxelles, Larcier, 2016, p. 523.

¹⁷⁶ L. STEVENS, *op.cit.*, p.850.

¹⁷⁷ Proposition de loi modifiant le Code pénal en vue de garantir la protection pénale des enfants contre le « *grooming* » (mise en confiance à des fins d’abus sexuel), Développements, *op.cit.*, p. 11.

¹⁷⁸ O. LEROUX, « Section 2. - Criminalité informatique aspécifique », *op.cit.*, p. 523.

¹⁷⁹ Proposition de loi modifiant le Code pénal en vue de garantir la protection pénale des enfants contre le « *grooming* » (mise en confiance à des fins d’abus sexuel), Développements, *op.cit.*, p. 11.

¹⁸⁰ O. LEROUX, « Section 2. - Criminalité informatique aspécifique », *op.cit.*, p. 523.

¹⁸¹ *Ibid.*

¹⁸² J.-F. HENROTTE et F. JONGEN, *op.cit.*, p. 235.

¹⁸³ C. pén., art. 377^{quater}.

Chapitre III. Publicité d'offre à caractère sexuel sur Internet et responsabilité des plateformes numériques

Afin de lutter efficacement contre la « composante numérique » de la traite des êtres humains, les instruments juridiques doivent pouvoir couvrir différentes étapes de la cybercriminalité¹⁸⁴ et éventuellement imposer des sanctions à différents acteurs. C'est pourquoi nous nous penchons, dans ce chapitre, sur la responsabilité pénale des plateformes numériques pour du contenu relatif à des cas de traite sexuelle.

Section I. La publicité d'offres à caractère sexuel sur Internet

Si la prostitution en elle-même n'est pas interdite en droit belge, la publicité de la prostitution est sanctionnée par l'article 380ter du Code pénal. Cet article ne punit ni le service sexuel, ni l'offre mais bien la publicité qui en est faite.

Le paragraphe premier de l'article 380ter punit « quiconque, quel qu'en soit le moyen, fait ou fait faire, publie, distribue ou diffuse de la publicité, de façon directe ou indirecte, même en en dissimulant la nature sous des artifices de langage, pour une offre de services à caractère sexuel, lorsque cette publicité s'adresse spécifiquement à des mineurs ou lorsqu'elle fait état de services proposés soit par des mineurs, soit par des personnes prétendues telles ».

En se référant à « quiconque » le législateur entend punir une large catégorie de personnes¹⁸⁵, tant « les auteurs matériels (celui qui fait, distribue ou diffuse) que les auteurs moraux (celui qui fait faire) et au même titre les personnes qui « de façon directe ou indirecte » accomplissent ces actes »¹⁸⁶. Le Code pénal ne définit pas la notion de « service à caractère sexuel ». Ce choix a été justifié par le législateur de 1995¹⁸⁷ par la nécessité de conférer à la notion un caractère évolutif¹⁸⁸. La publicité doit viser spécifiquement mais pas exclusivement des mineurs ou faire état de services proposés par des mineurs, même si en réalité ce n'est pas le cas¹⁸⁹.

¹⁸⁴ F. DECHAMPS et C. LAMBILOT, *op.cit.*, p.25.

¹⁸⁵ C.-E. CLESSE, *La traite des êtres humains - Droit belge éclairé des législations française, luxembourgeoise et suisse, op.cit.*, p. 645.

¹⁸⁶ A. DE NAUW, *Initiation au droit pénal spécial*, Waterloo, Kluwer, 2008, pp. 227-228.

¹⁸⁷ Loi du 27 mars 1995 insérant un article 380quinquies dans le Code pénal et abrogeant l'article 380quater, alinéa 2, du même Code, *M.B.*, 25 avril 1995, p.10822.

¹⁸⁸ Projet de loi insérant un article 380quinquies dans le code pénal et abrogeant l'article 380quater, deuxième alinéa, du même Code, Rapport fait au nom de la commission de la justice, *Doc. parl.*, Sén., sess. ord. 1994-1995, n° 1246/2, p. 11.

¹⁸⁹ C.-E. CLESSE, C.-E. CLESSE, *La traite des êtres humains - Droit belge éclairé des législations française, luxembourgeoise et suisse, op.cit.*, p. 646.

Le second paragraphe concerne la publicité d'offres à caractère sexuel, lorsque ces services sont fournis par un moyen de télécommunication. Avant son abrogation par la loi du 13 juin 2005¹⁹⁰, l'article 68, 4° de la loi du 21 mars 1991 définissait les moyens de télécommunication comme « toute transmission, émission, ou réception de signes, signaux, d'écrits, d'images, de son, données de toute nature par fil, radioélectricité, signalisation optique ou un autre système électromagnétique ». Les mineurs ne sont plus spécifiquement visés, l'offre peut concerner des mineurs comme des majeurs¹⁹¹. Il faut préciser que ce qui est visé par ce deuxième paragraphe ce n'est pas le mode de communication de l'offre (la loi précise « quel qu'en soit le moyen »), mais bien le mode par lequel les services sexuels seront fournis¹⁹². À l'origine, cette disposition visait notamment les lignes téléphoniques dites érotiques ou de téléphone rose. De par sa rédaction générale cette disposition est également applicable à la publicité pour des services sexuels proposés via Internet (offre de sexe virtuel).

Le dernier paragraphe s'applique généralement à toute publicité « résiduaire » pour une activité de prostitution, dès lors que cette publicité n'est pas visée par un autre paragraphe de l'article 380ter¹⁹³. Le champ d'application de ce dernier paragraphe est très large de sorte qu'il englobe toute forme de support publicitaire, dont les annonces postées sur Internet¹⁹⁴.

La Cour de Cassation, dans son arrêt du 20 novembre 2001¹⁹⁵ a précisé que l'incrimination de l'article 380ter s'appliquait tant à la publicité pour la prostitution organisée liée à l'exploitation sexuelle qu'à celle pour la simple prostitution volontaire et individuelle, qui n'est pas punissable en soi. Par ailleurs, lorsqu'il est question de publicité faisant état de services proposés par des mineurs, la loi prévoit une aggravation de la peine lorsque cette publicité a pour objet ou pour effet de faciliter la prostitution ou la débauche d'un mineur ou son exploitation à des fins sexuelles¹⁹⁶.

¹⁹⁰ Loi du 13 juin 2005 relative aux communications électroniques, *M.B.*, 20 juin 2005, p.28070.

¹⁹¹ *Ibid.*, p. 647.

¹⁹² O. LEROUX, « La corruption de la jeunesse et les outrages publics aux bonnes mœurs par courrier électronique (courriel, SMS, MMS) », *R.D.T.I.*, n°17/2003, p. 18.

¹⁹³ P. MONVILLE et D. HOLZAPFEL, « La prostitution, le droit pénal dans une drôle de posture... », in *Omniprésence du droit pénal. Nouvelles approches pluridisciplinaires* (sous la dir. de N. RADELET), Limal, Anthemis, 2017, p. 20.

¹⁹⁴ *Ibid.*

¹⁹⁵ Cass., 20 novembre 2001, *Pas.*, 2001, II, p. 1906.

¹⁹⁶ C. pén., Art. 380bis, §1^{er}, al.2.

La publicité pour une offre de services à caractère sexuel est interdite, même si elle est dissimulée sous des artifices de langage. Il en résulte que « toute publicité relative à une activité de prostitution est sanctionnée pénalement, même si elle est faite de manière plus ou moins détournée, sans faire état ouvertement du service vanté, pour peu qu'il n'y ait aucun doute sur celui-ci »¹⁹⁷. Sur Internet, les petites annonces, les sites d'escortes, les rubriques « massages », ne font bien souvent aucune mention ni de prix ni de prestations explicites, mais de mots ou d'images évocatrices. Ce type d'offres tombent dans le champ d'application de l'article 380ter, et peuvent être sanctionnés sur cette base¹⁹⁸.

Concernant l'élément matériel, il s'agit d'un dol général¹⁹⁹. Il n'est pas requis que la publicité soit faite dans un but lucratif direct ou indirect²⁰⁰.

Section II. La responsabilité des prestataires intermédiaires

§1. Considérations préliminaires

L'auteur d'un contenu illégal sur Internet est le premier responsable pénalement²⁰¹. Si la responsabilité de celui qui a publié des annonces d'offres à caractère sexuel sur Internet est acquise dès lors qu'il a agi sciemment, les coauteurs et complices de telles infractions peuvent également faire l'objet de poursuites pénales. On songe alors à la responsabilité des plateformes numériques qui abritent ce contenu illégal.

Dans cette section nous entendons analyser la possible responsabilité des sites Internet relativement aux infractions contenues à l'article 380ter analysé ci-dessus. Précisons à ce stade et au besoin, que ces infractions peuvent ressortir de faits de traite des êtres humains, mais que ce n'est pas forcément toujours le cas. Les sites internet utilisés par les proxénètes pour vendre les services de leurs victimes sont les mêmes que ceux utilisés par les personnes se livrant volontairement à la prostitution²⁰². Ainsi, les publicités de services sexuels en ligne ne cachent pas toujours des victimes de traite.

¹⁹⁷ P. MONVILLE et D. HOLZAPFEL, *op.cit.*, p. 20.

¹⁹⁸ Dans des dossiers de traite sexuelle voy. par ex. Liège, 1er juin 2017, disponible sur : https://www.myria.be/files/h17-06-01_a_Li%C3%A8ge.pdf ou Corr. Liège (19^e ch.), 23 novembre 2016, disponible sur : https://www.myria.be/files/h16-11-16_Corr_Li+%C2%BFge.pdf.

¹⁹⁹ C.-E. CLESSE, *La traite des êtres humains - Droit belge éclairé des législations française, luxembourgeoise et suisse, op.cit.*, pp. 646-650.

²⁰⁰ Projet de loi relatif à la protection pénale des mineurs, Exposé des motifs, *Doc. Parl.*, Ch. repr., sess. ord. 1998-1999, n°1907/1, p.44.

²⁰¹ C. DE CALLATAÏ, « Les responsabilités liées aux messages postés sur internet : l'extension du régime d'exonération de responsabilité des intermédiaires aux acteurs du web 2.0 », *A&M*, 2013/3-4, p. 166.

²⁰² CONSEIL DE L'EUROPE, *Traite des êtres humains : recrutement par internet, op.cit.*, p.40.

§2. La directive e-commerce

La directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (dite « directive e-commerce »)²⁰³ règle les cas dans lesquels la responsabilité civile et pénale des prestataires de services sur Internet peut être retenue. Elle a été transposée en droit belge par la loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information²⁰⁴. Les dispositions contenues dans cette loi ont ensuite été insérées dans le Code de droit économique²⁰⁵. La directive se veut protectrice, immunisant ceux qui ne jouent qu'un rôle d'intermédiaire en prévoyant une exonération de leur responsabilité dans certains cas déterminés²⁰⁶.

§3. L'exonération de responsabilité des prestataires intermédiaires

A. Champ d'application

Précisons d'emblée que la directive introduit une absence d'obligation générale positive pour les intermédiaires de rechercher activement l'information illicite, ou de rechercher des faits ou circonstances révélant des activités illicites²⁰⁷. Si cette absence d'obligation de surveillance se justifiait assez bien lors de son entrée en vigueur en 2000, on peut se demander si tel est encore le cas aujourd'hui, compte tenu des évolutions techniques en matière de filtrage automatique²⁰⁸. La directive prévoit par ailleurs la possibilité d'instaurer pour les prestataires de services, l'obligation d'informer promptement les autorités publiques compétentes d'activités illicites alléguées qu'exerceraient les destinataires de leurs services ou d'informations illicites alléguées que ces derniers fourniraient ou de communiquer aux autorités compétentes, à leur demande, les informations permettant d'identifier les destinataires de leurs services avec lesquels ils ont conclu un accord d'hébergement²⁰⁹. La Belgique a fait usage de cette possibilité en prévoyant de telles obligations²¹⁰.

²⁰³ Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur, *J.O.C.E.*, 17 juillet 2000, L 178, p. 1 (ci-après « Directive e-commerce »).

²⁰⁴ Loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information, *M.B.*, 17 mars 2003, p.12963.

²⁰⁵ Par une loi du 15 décembre 2013 portant insertion du Livre XII, « Droit de l'économie électronique » dans le Code de droit économique, *M.B.*, 14 janvier 2014, p.1524.

²⁰⁶ C. DE CALLATAY, *op. cit.*, p. 166.

²⁰⁷ Directive e-commerce, art. 15, al. 1^{er}.

²⁰⁸ R. HARDOUIN, « La connaissance de l'illicéité par les hébergeurs ou quand être notifié ne signifie pas nécessairement devoir retirer », *R.D.T.I.*, 2012/2, n° 47, p. 10.

²⁰⁹ Directive e-commerce, art. 15, al. 2.

²¹⁰ C.D.E., art. XII. 20 §2.

La directive instaure un régime d'exonération pour trois catégories d'activités : le transport, le stockage (« *caching* ») et l'hébergement. C'est en effet la nature des activités d'un prestataire et non sa qualité qui conditionne l'application du régime d'exonération²¹¹. Ces activités ont pour point commun de présenter un certain degré de neutralité, c'est-à-dire qu'elles requièrent un comportement purement technique, automatique et passif²¹². D'autres activités telles que la production ou l'édition ne sont pas visées et sont soumises au droit commun de la responsabilité²¹³. L'exonération concerne tant la responsabilité civile que la responsabilité pénale des prestataires intermédiaires. Elle s'applique « de manière horizontale, peu importe la nature de l'activité illicite et les dispositions légales ou réglementaires violées »²¹⁴. En outre, elle couvre les situations où le prestataire a commis lui-même une infraction (qualité d'auteur), mais également lorsqu'il a apporté une aide à la réalisation d'une infraction commise par une autre personne (qualité de coauteur ou de complice)²¹⁵.

B. Conditions

Les prestataires de services de « simple transport » sont exemptés de responsabilité lorsque le prestataire de services ne joue qu'un rôle passif dans la transmission des données²¹⁶.

Les prestataires de stockage sont pareillement exemptés lorsqu'ils stockent des données de manière automatique et temporaire dans le seul but de rendre plus efficace la transmission, sous certaines conditions²¹⁷.

L'activité d'hébergement a donné lieu à plus de réflexions doctrinales et jurisprudentielles. En effet, la directive a été adoptée à un moment où « on ne se doutait pas encore de l'essor du web 2.0 »²¹⁸ et la question s'est alors posée de savoir si le régime de responsabilité des hébergeurs prévu par la directive s'étendait aux réseaux sociaux et autres sites collaboratifs sur lesquels du

²¹¹ H. JACQUEMIN, « Responsabilité et numérique : le régime d'exonération de responsabilité des prestataires intermédiaires », *For. Ass.*, 2018/9, n° 188, p. 178.

²¹² *Ibid.*

²¹³ E. MONTERO, M. DEMOULIN et CH. LAZARO, « La loi du 11 mars 2003 sur les services de la société de l'information », *J.T.*, 2004, p. 92.

²¹⁴ H. JACQUEMIN, *op.cit.*, p. 179.

²¹⁵ E. MONTERO, M. DEMOULIN et CH. LAZARO, *op.cit.*, p.92.

²¹⁶ Directive e-commerce, art. 12.

²¹⁷ Directive e-commerce, art.13.

²¹⁸ C. DE CALLATAÏ, *op. cit.*, p. 167 ; Par « Web 2.0 » nous entendons le passage pour les utilisateurs d'une utilisation passive et consultative d'Internet à une utilisation interactive avec la possibilité d'en déterminer le contenu.

contenu peut être posté par des internautes²¹⁹. La jurisprudence européenne a depuis lors répondu à cette question par l’affirmative²²⁰. Il en résulte que « le prestataire du web 2.0 est souvent dans une position ambivalente : il est à la fois éditeur à raison de l’architecture choisie pour le site, des rubriques proposées, et hébergeur au regard de l’activité de stockage des annonces, messages, commentaires postés par ses utilisateurs »²²¹.

L’hébergeur a davantage de responsabilité que tout autre intermédiaire²²² mais bénéficie toutefois d’un régime de responsabilité allégé puisque sa responsabilité ne peut en principe pas être engagée à deux conditions²²³. Pour être exonéré, l’intermédiaire qui héberge du contenu ne peut avoir une connaissance effective du contenu (qui résultait par exemple d’une notification de la présence du contenu illicite), ou indirecte (à travers des faits laissant présumer le caractère illicite du contenu)²²⁴. Si la connaissance du contenu est établie, l’intermédiaire ne sera exonéré que s’il agit rapidement pour enlever ou bloquer l’accès à l’information illicite²²⁵.

À propos de ces conditions, nous constatons qu’en droit belge aucune procédure n’est légalement prévue pour organiser la notification d’une illicéité par un utilisateur du service²²⁶. De plus, le seuil de connaissance requis pour écarter l’exonération est une question délicate. La question se pose de savoir si la connaissance doit porter uniquement sur l’existence de l’infraction ou également sur son caractère illicite, dans ce dernier cas, cette exigence reviendrait à faire endosser à l’intermédiaire un rôle de juge pour lequel il n’est pas forcément compétent²²⁷. La directive n’apporte pas de précisions suffisantes sur ce point.

Précisons que l’intermédiaire qui ne satisferait pas à ces conditions et qui ne bénéficierait donc pas de l’exonération ne serait pas pour autant *ipso facto* responsable pénalement du fait du

²¹⁹ H. JACQUEMIN, *op.cit.*, p. 179.

²²⁰ C.J.U.E., 23 mars 2010 (Google France et Google c. Louis Vuitton Malletier), Aff. jointes C-236/08 à C-238/08, EU:C:2010:159, point 111 ; C.J.U.E., 12 juillet 2011 (L’Oréal SA et autres contre eBay International AG et autres), EU:C:2011:474, point 110 ; C.J.U.E., 16 février 2012 (SABAM c. Netlog), C-360/10, EU:C:2012:85:1036, point 27.

²²¹ C. DE CALLATAÏ, *op. cit.*, p. 167.

²²² C. FORGET, « Chapitre 6 - Méthodes d’enquête pénales et protection des personnes vulnérables dans l’environnement numérique » in *Vulnérabilités et droits dans l’environnement numérique*, *op.cit.*, p. 182.

²²³ Directive e-commerce, art.14.

²²⁴ C.D.E., art. XII. 19 §1^{er}, 1^o ; F. JONGEN et A. STROWEL, *Droit des médias et de la communication*, Bruxelles, Larcier, 2017, pp. 787-788.

²²⁵ C.D.E., art. XII. 19, § 1, 2^o ; *Ibid.*, p. 788.

²²⁶ H. JACQUEMIN, *op.cit.*, p. 180.

²²⁷ F. JONGEN et A. STROWEL, *op. cit.*, p. 787.

contenu illicite²²⁸. Encore faut-il que les éléments constitutifs de l'infraction de la publicité d'offres à caractère sexuel (380ter) soient réunies. Nous rappelons que l'élément moral de cette infraction correspond à un dol général.

Par ailleurs, nous n'avons trouvé en droit belge qu'une seule décision relative à la responsabilité des intermédiaires. L'arrêt du 3 février 2004 de la Cour de Cassation²²⁹ concernait un webmaster condamné du fait d'hyperliens renvoyant vers des sites abritant du matériel pédopornographique, postés sur son site par des utilisateurs. La Cour avait estimé que l'individu ne pouvait se prévaloir de la qualité d'intermédiaire car il avait connaissance des contenus²³⁰. Cette décision est toutefois d'un intérêt limité, puisque la Cour y a confondu le concept de « prestataire intermédiaire » avec les conditions de l'exonération prévues par la directive²³¹.

C. En pratique

En ce qui concerne la publicité d'offres à caractère sexuel, des sites Internet peuvent être créés par les criminels dans des pays où la législation ne les interdit pas. En effet, contrairement à l'incrimination de la pédopornographie, il n'existe pas en la matière de législation harmonisée en Europe et encore moins à l'international.

Il semble peu probable qu'un site comme Quartierrouge.be²³², qui se décrit lui-même comme la plateforme d'hébergement n°1 en Belgique pour les annonces d'escorte, ignore le caractère illicite du contenu qu'il abrite. Selon les conditions de la directive, la responsabilité de ce genre de sites spécialisés pourrait être engagée. Nous n'avons pourtant trouvé aucune décision en ce sens en jurisprudence.

Ceci s'explique probablement par le fait que autorités judiciaires belges tolèrent largement ce type de publicité en ligne²³³. Le SPF Justice indique d'ailleurs à ce sujet que : « *Eu égard au*

²²⁸ H. JACQUEMIN, *op.cit.*, p. 179.

²²⁹ Cass., (2^e ch.), 3 février 2004, *Pas.*, 2004, I, p. 200.

²³⁰ D. FESLER et E. DEHARENG, « La responsabilité des hébergeurs et des intermédiaires au regard du développement des services en ligne » in *Le droit des nouvelles technologies et de l'internet*, Bruxelles, Bruylant, 2012, p. 72.

²³¹ C. DE CALLATAÏ, *op. cit.*, p. 168.

²³² Conscients que leur site peut être utilisé à des fins d'exploitation sexuelle le site indique que: « le trafic d'êtres humains, la prostitution forcée et la prostitution d'enfants sont absolument pas toléré! Malheureusement, il ne nous est pas toujours possible, en tant que plate-forme d'annonce, de reconnaître les abus sur base d'une annonce ou d'un profil ».

²³³ P. MONVILLE et D. HOLZAPFEL, *op.cit.*, p. 20.

principe de l'opportunité des poursuites applicable en Belgique, le ministère public n'est pas obligé de poursuivre toutes les infractions dont il a connaissance et il établit des priorités en respectant les directives générales du Collège des Procureurs généraux, notamment en matière de traite des êtres humains. (...) Appliquer l'art. 380ter de manière conséquente et ensuite fermer tous ces sites n'est ni réaliste ni opportun. Ils continueront à apparaître (se déplaçant au besoin vers des pays plus tolérants) et la prostitution s'exercera davantage dans la clandestinité. Cela compliquera davantage les possibilités d'identifier les cas d'exploitation sexuelle »²³⁴. Plus encore, le SPF indique que : « ces sites internet communiquent des informations aux parquets sur des annonces qu'ils soupçonnent couvrir des faits d'exploitation, ce qui peut donner lieu à l'ouverture d'enquêtes et à des poursuites. Sur une simple requête par une apostille, ils fournissent toutes les données utiles et vraiment exploitables pour permettre l'identification des auteurs. Ces sites déclarent eux-mêmes ne pas tirer de profit commercial en cas d'abus perpétré via leur site internet, et plusieurs dénonciations spontanées sont déjà venues d'eux ».

§4. D'hébergeur à éditeur : Le cas Vivastreet en France

Selon la jurisprudence de la Cour de Justice de l'Union européenne, la directive ne protège que le prestataire intermédiaire « neutre, en ce que son comportement est purement technique, automatique et passif, impliquant l'absence de connaissance ou de contrôle des données qu'il stocke »²³⁵, ce qui n'est pas le cas des éditeurs de contenu²³⁶.

Il semble que la tolérance belge ne soit pas de mise partout. En France la plateforme *Vivastreet*, un site d'annonces généraliste qui opère également en Belgique, a été accusée de proxénétisme aggravé en raison d'annonces plus ou moins suggestives dans certaines rubriques du site²³⁷. La plateforme se défend en arguant que, en tant hébergeur, elle ne saurait être tenue responsable du contenu posté par des tiers²³⁸. Or il s'avère que la plateforme rééditorialise certains contenus et propose un service payant permettant d'optimiser des annonces. De ce fait, elle pourrait être considérée comme un éditeur, qui ne bénéficie pas de la protection de la directive. En effet,

²³⁴ RTL Info, « Le site de petites annonces Vivastreet.be, plateforme de prostitution ? Le fondateur se défend », 31 mai 2018, disponible sur www.rtl.be.

²³⁵ C.J.U.E., 23 mars 2010 (Google France et Google c. Louis Vuitton Malletier), Aff. jointes C-236/08 à C-238/08, EU:C:2010:159, point 112 et 113.

²³⁶ C. FORGET, « Chapitre 6 - Méthodes d'enquête pénales et protection des personnes vulnérables dans l'environnement numérique », *op.cit.*, p. 185.

²³⁷ Le Figaro, « Vivastreet poursuivi pour "proxénétisme aggravé" », 31 mai 2018, disponible sur www.lefigaro.fr.

²³⁸ A. BEELEN, C. CHARLIER et J. VIGNERON, *Guide pratique des plateformes*, Bruxelles, Larcier, 2021, p. 148.

dans son arrêt l'Oréal c. eBay du 12 juillet 2011²³⁹, la Cour de Justice de l'Union européenne a jugé qu'un exploitant qui « a prêté une assistance laquelle a notamment consisté à optimiser la présentation des offres à la vente en cause ou à promouvoir ces offres, il y a lieu de considérer qu'il a non pas occupé une position neutre entre le client vendeur concerné et les acheteurs potentiels, mais joué un rôle actif de nature à lui conférer une connaissance ou un contrôle des données relatives à ces offres. Il ne saurait alors se prévaloir, s'agissant desdites données, de la dérogation en matière de responsabilité visée à l'article 14 de la directive 2000/31»²⁴⁰.

En conséquence, l'opérateur est responsable de plein droit des annonces qu'il éditorialise, sur le plan civil comme pénal²⁴¹. Tel pourrait bien être le cas du site d'annonces *Vivastreet*²⁴².

§5. Les lois FOSTA/SESTA aux États-Unis : un exemple à suivre ou ne pas suivre ?

Les lois FOSTA (« *Allow States and Victims to Fight Online Sex Trafficking Act* ») et SESTA (« *Stop Enabling Sex Traffickers Act* ») ont été adoptées en avril 2018, suite à une longue période d'impunité pour les sites mettant sciemment en avant des annonces à caractère prostitutionnel ou cachant des activités d'exploitation sexuelle aux États-Unis²⁴³. L'article 230 du *Communications Decency Act*²⁴⁴ (CDA) garantissait aux sites Internet une large immunité civile et pénale pour le contenu posté par des tiers²⁴⁵. Un site d'annonces en particulier, *Backpackage* était accusé de faciliter et d'encourager la traite sexuelle des enfants en connaissance de cause, tout en étant protégé par le bouclier que représentait l'immunité de l'article 230 du CDA²⁴⁶. La loi a été modifiée pour permettre de poursuivre les sites Internet qui en connaissance de cause assistent, supportent ou facilitent la traite des êtres humains²⁴⁷ en postant les annonces de proxénètes et de trafiquants. Ce nouveau cadre législatif a été critiqué pour différentes raisons. Certains accusent la loi d'amalgamer les phénomènes prostitution et

²³⁹ C.J.U.E, 12 juillet 2011 (L'Oréal SA et autres contre eBay International AG et autres), EU:C:2011:474.

²⁴⁰ C.J.U.E, 12 juillet 2011 (L'Oréal SA et autres contre eBay International AG et autres), EU:C:2011:474, point 116.

²⁴¹ A. BEELEN, C. CHARLIER et J. VIGNERON, *op.cit.*, p.148.

²⁴² FONDATION SCÉLLES, 5^e Rapport mondial, *Système prostitutionnel - Nouveaux défis, nouvelles réponses*, 2019, p.34, disponible sur : <https://www.fondationscelles.org/>.

²⁴³ E. M. DONOVAN, « Fight Online Sex Trafficking Act and Stop Enabling Sex Traffickers Act: A Shield for Jane Doe », *Connecticut Law Review*, 2020, p.88.

²⁴⁴ Telecommunications Act of 1996, Pub. L. No. 104-104, tit. V (1996).

²⁴⁵ L'article 230 indique que: « No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider ».

²⁴⁶ M. MCKNELLY, « Untangling SESTA/FOSTA: How the Internet's 'Knowledge' Threatens Anti-Sex Trafficking Law », *Berkeley Technology Law Journal*, 2019, pp. 1244-1245.

²⁴⁷ K.M. PRYLINSKI, « Tech Trafficking: How the internet has transformed sex trafficking », *Journal of High Technology Law*, 2020, p.353.

traite des êtres humains²⁴⁸. D'autres s'inquiètent du possible effet contre-productif que peuvent avoir ces nouvelles dispositions, dans la mesure où elles peuvent pousser les criminels à agir de manière plus clandestine et rendre la détection des victimes plus difficile.

§6. Conclusion

Pour notre part, nous nous rallions à la position belge en la matière. Nous ne pensons pas que la poursuite systématique des sites Internet soit une solution satisfaisante pour contrer l'usage d'Internet par les trafiquants pour exploiter leurs victimes. Nous plaçons plutôt pour une collaboration accrue avec ces plateformes afin d'identifier les auteurs et de détecter plus efficacement de potentielles victimes. En outre, il semble que les règles instaurées par la directive il y a maintenant plus de 20 ans n'ont pas permis d'instaurer un régime clair pour la responsabilité des plateformes numériques, particulièrement pour les acteurs du Web 2.0²⁴⁹ rendant la possibilité d'engager leur responsabilité incertaine. La jurisprudence développée par la Cour de Justice de l'Union européenne axée autour du critère de neutralité ne fournit pas d'orientations suffisantes de sorte que la directive a donné lieu à des applications très variables dans les différents États membres. Sur ce point il convient de noter qu'une réforme est actuellement en cours au niveau européen pour clarifier le régime de responsabilité des intermédiaires en ligne²⁵⁰. Nous pensons en revanche qu'il est important que les sites concernés reconnaissent que leurs plateformes peuvent être utilisées par des trafiquants, et qu'ils mettent en place des mécanismes de signalement que peuvent utiliser leurs utilisateurs pour dénoncer des abus²⁵¹ comme c'est le cas de *Facebook*²⁵². Pour ce faire, il est nécessaire d'informer les utilisateurs de ces sites afin qu'ils puissent identifier des signes d'exploitation en ligne. À titre d'exemple, le site Quartier rouge que nous avons mentionné indique à ses utilisateurs des signaux qui pourraient indiquer des cas d'exploitation et invite ses utilisateurs à le leur signaler, ou à le signaler à la police.

²⁴⁸ Voy. H. TRIPP, « All sex workers deserve protection: How fosta/sesta overlooks consensual sex workers in an attempt to protect sex trafficking victims », *Penn State Law Review*, 2019, pp. 219-246.

²⁴⁹ Voy. not. C. CALLATAÏ, *op.cit.*, pp. 168-182 ; B. DOCQUIR, *Droit du numérique*, Bruxelles, Larcier, 2018, p. 575 ; T. LEONARD, « 4 - Les réseaux sociaux face à l'exonération de responsabilité des intermédiaires de l'internet : une application délicate » in *Les réseaux sociaux et le droit* (sous la dir. de M. SALMON), *op.cit.*, 2014, pp. 123-150.

²⁵⁰ PARLEMENT EUROPÉEN, *Réforme du régime européen de responsabilité des intermédiaires en ligne – Contexte de la future législation relative aux services numériques*, mai 2020, disponible sur [https://www.europarl.europa.eu/RegData/etudes/IDAN/2020/649404/EPRS_IDA\(2020\)649404_FR.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2020/649404/EPRS_IDA(2020)649404_FR.pdf).

²⁵¹ TRACE, *Report on the role of current and emerging technologies in human trafficking*, 2015, pp.79-80, disponible sur https://humantraffickingsearch.org/wp-content/uploads/2017/07/TRACE_D4.1_Role-of-technologies-in-human-trafficking_FINAL.-1.pdf.

²⁵² Voy. Facebook's Anti-Slavery and Human Trafficking Statement: [https://s21.q4cdn.com/399680738/files/doc_downloads/2020/06/2020-Facebook's-Anti-Slavery-and-Human-Trafficking-Statement-\(FINAL\).pdf](https://s21.q4cdn.com/399680738/files/doc_downloads/2020/06/2020-Facebook's-Anti-Slavery-and-Human-Trafficking-Statement-(FINAL).pdf).

Section IV. Le blocage des sites

La mesure de blocage de sites Internet n'est pas spécifiquement réglementée mais repose sur la saisie de données informatiques visée à l'article 39*bis* du Code d'instruction criminelle. Selon cette disposition, le procureur du Roi peut rendre inaccessibles les données formant l'objet de l'infraction, produites par l'infraction ou contraires à l'ordre public et aux bonnes mœurs²⁵³.

Ainsi, 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 39*bis*²⁵⁴. 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 informations²⁵⁵.

²⁵³ C.I.Cr, art. 39*bis* §6.

²⁵⁴ C.D.E., art. XII. 19, §3, al.1^{er}.

²⁵⁵ C.D.E., art. XII.19, §3, al.2.

Titre II. Les moyens d'enquête pour lutter contre l'usage d'Internet dans la traite à des fins d'exploitation sexuelle

Cette partie de notre travail est consacrée à l'analyse des mesures d'enquête qui existent pour exploiter les traces laissées par l'usage d'Internet dans les situations identifiées ; c'est-à-dire le recrutement des personnes majeures et mineures par Internet et l'offre de services sexuels des victimes sur Internet. Dans un premier temps nous nous intéressons au cadre légal entourant la recherche policière dans les sources ouvertes (Chapitre I). Nous abordons ensuite les conditions dans lesquelles des recherches peuvent être menées dans les smartphones ou autres appareils électroniques des trafiquants et des victimes (Chapitre II). Nous finissons par nous attarder sur un point qui nous semble essentiel à la lutte contre la traite des êtres humains via Internet, c'est-à-dire la collaboration des entreprises privées à l'enquête pénale (Chapitre III).

Chapitre I. La recherche policière dans les sources ouvertes

Les informations disponibles sur les réseaux sociaux et autres pages accessibles à tout utilisateur d'Internet peuvent constituer des éléments de preuve importants pour les enquêteurs. Le GRETA²⁵⁶ indique d'ailleurs qu'en Belgique « les unités de police spécialisées utilisent systématiquement Internet pour collecter des informations supplémentaires au cours des enquêtes pour traite, y compris Google, les réseaux sociaux et les forums. Les enquêteurs recherchent aussi des annonces, des publicités et des offres d'emplois ou de services qui pourraient révéler des cas d'exploitation éventuels »²⁵⁷. Ainsi, dans les dossiers de traite, la recherche dans les sources ouvertes constitue une partie importante du travail policier²⁵⁸.

Section I. Patrouiller sur Internet de manière proactive

§1. Sources ouvertes sur Internet

Les sites Internet accessibles via des moteurs de recherche comme Google sont appelés « sources ouvertes » dans la mesure où n'importe quel utilisateur peut y avoir accès²⁵⁹. Selon

²⁵⁶ Le groupe d'experts sur la lutte contre la traite des êtres humains (GRETA) assure le suivi de la mise en œuvre de la Convention du Conseil de l'Europe par les États parties.

²⁵⁷ GRETA, *Rapport concernant la mise en œuvre de la Convention du Conseil de l'Europe sur la lutte contre la traite des êtres humains par la Belgique*, 2017, p.46, disponible sur : <https://rm.coe.int/2nd-rd-rpt-bel/1680766bdb>.

²⁵⁸ MYRIA, *Rapport annuel traite et trafic des êtres humains*, 2017, p.48., disponible sur : <https://www.myria.be/files/RA-TEH-17.pdf>.

²⁵⁹ C. FORGET, « La collecte de preuves sur le *darknet* et les espaces accessibles au public », note sous Cass., 28 mars 2017, *Rev. Dr. Pén. Crim.*, p.706.

l'article 32 a) de la Convention sur la cybercriminalité²⁶⁰ les enquêteurs peuvent accéder à ces données informatiques stockées accessibles au public, et ce quelle que soit la localisation géographique de ces données.

§2. L'enquête proactive

Les recherches sur Internet par les services de police s'effectuent souvent dans le cadre d'une enquête déjà ouverte, de manière réactive suite au témoignage d'une victime par exemple. Mais elles peuvent aussi être menées de manière proactive car « la traite des êtres humains constitue l'un des rares délits dans le cadre desquels il faut rechercher activement les victimes, ce que permettent les nouvelles technologies »²⁶¹. En 2010 déjà, *Myria*²⁶² indiquait la nécessité d'assurer une surveillance systématique de sites proposant des services sexuels et offres d'emploi afin d'y déceler des indicateurs de traite²⁶³.

L'article 28bis §2 du Code d'instruction criminelle (C.I.Cr) consacre la figure de l'enquête proactive²⁶⁴ en droit belge. Cette dernière « consiste en la recherche, la collecte, l'enregistrement et le traitement de données et d'informations sur la base d'une suspicion raisonnable que des faits punissables vont être commis ou ont été commis mais ne sont pas encore connus ». Une enquête proactive ne peut être menée pour n'importe quels faits. Ceux-ci doivent relever d'une organisation criminelle, ou constituer un crime ou délit visé par l'article 90ter §2 à 4 du Code d'instruction criminelle, ce qui est le cas de la traite des êtres humains. Pour entamer une enquête proactive, une autorisation du procureur du Roi est nécessaire.

Section II. Cadre légal

§1. L'arrêt du 28 mars 2017 de la Cour de Cassation

Comme tout autre utilisateur, la police peut consulter des sites Internet accessibles au public, pour prendre connaissance de leur contenu et éventuellement d'en assurer une copie²⁶⁵. Dans

²⁶⁰ Convention sur la cybercriminalité, signée à Budapest le 23 novembre 2001, approuvée par la loi du 3 août 2012, *M.B.*, 21 novembre 2012, p.69092.

²⁶¹ ASSEMBLÉE INTERPARLEMENTAIRE BENELUX, Session 2019, Séances plénières des 14 et 15 juin 2019, compte rendu analytique des réunions, *Débat thématique sur la Traite des êtres humains et les technologies innovantes en vue de lutter contre la traite des êtres humains*, p. 23.

²⁶² Myria est le Centre fédéral Migration. Il a notamment pour but de stimuler la lutte contre le trafic et la traite des êtres humains.

²⁶³ MYRIA, *Rapport annuel traite et trafic des êtres humains*, 2010, *op.cit.*, p.116.

²⁶⁴ C. DE VALKENEER, *Manuel de l'enquête pénale*, Bruxelles, Éditions Larcier, 2018, p. 16.

²⁶⁵ M. GIACOMETTI et P. MONVILLE, *op.cit.*, p. 189.

un arrêt du 28 mars 2017²⁶⁶ la Cour de Cassation a rappelé qu'en vertu de l'article 26 de la loi sur la fonction de police²⁶⁷ les officiers de police judiciaire peuvent consulter les données sur un site Internet accessible au public afin de rechercher les crimes, délits et contraventions et de rassembler des preuves afin de livrer les auteurs aux tribunaux chargés de les punir²⁶⁸. L'article 26 de la loi sur la fonction de police stipule que : « Les fonctionnaires de police peuvent toujours pénétrer dans les lieux accessibles au public ainsi que dans les biens immeubles abandonnés, afin de veiller au maintien de l'ordre public et au respect des lois et des règlements de police. Ils peuvent toujours pénétrer en ces mêmes lieux afin d'exécuter des missions de police judiciaire ».

Précisons que dans cet arrêt, la Cour se prononçait sur le pouvoir des services de police de recueillir des preuves sur le *darknet*²⁶⁹. Les avantages ce type de réseau en ont fait un choix privilégié par les criminels pour perpétrer toutes sortes d'activités illicites : trafic de drogues, vente d'armes mais aussi traite des êtres humains. L'utilisation du *darkweb* est moins intéressante pour les trafiquants dans la phase de recrutement ou d'exploitation de personnes majeures puisqu'ils cherchent à ce que leur publications soient visible au plus grand nombre, en revanche elle l'est beaucoup plus en cas d'exploitation sexuelle des enfants²⁷⁰. Le *darknet* peut être utilisé pour vendre ouvertement les services sexuels de victimes mineures. L'assurance d'anonymat (des trafiquants et des clients) garantit un faible risque d'être détecté par les autorités répressives²⁷¹.

§2. Lieu accessible au public dans un contexte numérique

Le recours à l'article 26 de la loi sur la fonction de police pour justifier le pouvoir de la police d'enquêter dans les sources ouvertes, qui avait antérieurement été suggéré par la doctrine²⁷², repose sur un parallélisme entre les lieux accessibles au public dans le monde physique et les données accessibles au public dans un monde virtuel. La Cour précise à propos de la notion d'« accessible au public », que cela vise un accès qui est possible « sans contrôle réel ou sans

²⁶⁶ Cass. (2^e ch.), 28 mars 2017, *Pas.*, 2017/3, p. 759.

²⁶⁷ Loi du 5 août 1992 sur la fonction de police, *M.B.*, 22 décembre 1992, p.27124.

²⁶⁸ C.I.Cr, art. 8.

²⁶⁹ Le terme « *darknet* » renvoie à un réseau virtuel anonymisant les utilisateurs et les données. Ce type de réseau n'implique pas de partage des adresses IP.

²⁷⁰ ASSEMBLÉE INTERPARLEMENTAIRE BENELUX, *op.cit.*, p.30.

²⁷¹ SURF AND SOUND, *Improving and sharing knowledge on the Internet role in the processes of human trafficking and smuggling*, 2017, p.98, disponible sur <http://www.surfandsound.eu/>.

²⁷² C. CONINGS et P. VAN LINTHOUT, « Sociale media – Een nieuwe uitdaging voor politie en justitie », *Panopticon*, 2012, vol. 3, pp. 218-219.

vérification sur la qualité des personnes ». Elle indique également que le fait que la visite d'un site soit subordonnée à des conditions d'accès purement formelles n'est pas de nature à conférer à un site la caractéristique d'être inaccessible au public. Ceci implique que lorsqu'un site Internet n'est pas limité à un cercle privé, la police peut le visiter sans autorisation particulière, même si l'accomplissement de certaines formalités a été nécessaire. En effet, selon la Cour de Cassation, « l'utilisation d'un alias peut relever du mode normal de la consultation de pages d'internet, sous réserve que cette utilisation ne consiste pas à endosser une identité fictive plausible et que l'alias utilisé n'est pas de nature à provoquer la commission d'une infraction ».

§3. Conditions de mise en œuvre

Le pouvoir de mener des recherches dans des sources ouvertes n'est donc pas prévu par une loi spécifique²⁷³ mais repose sur une disposition générale. Pour autant cette consultation suppose le respect de certaines garanties²⁷⁴. Pour l'accomplissement de missions judiciaires la police peut pénétrer les « lieux » si une infraction existe au préalable ou si elle n'a pas été constatée, qu'il existe des indices qu'une infraction va être commise²⁷⁵. Cela signifie que la police ne peut se livrer à des recherches exploratoires²⁷⁶. De plus les officiers de police judiciaire qui auraient pris l'initiative de mener des recherches sur Internet doivent en informer le Procureur du roi²⁷⁷.

L. Beirens indique par contre que la recherche exploratoire d'éventuelles activités criminelles sur Internet, sans qu'il y ait déjà d'indications concrètes que des infractions ont été commises ou sont sur le point de l'être, est autorisée dans le cadre d'une enquête proactive pour laquelle le ministère public a donné son accord écrit préalable. Une telle enquête doit être limitée dans le temps et avoir des objectifs clairement définis²⁷⁸.

§4. Un besoin de clarification

La justification de ces pouvoirs par une base légale générale et l'absence d'encadrement strict génèrent des inquiétudes quant au risque d'ingérence dans le droit au respect de la vie privée des personnes concernées. Dans son arrêt du 28 mars 2017 la Cour de cassation n'a pas pris le soin de définir plus précisément la notion de « lieu accessible au public » dans un contexte

²⁷³ C. FORGET, « La collecte de preuves sur le *darknet* et les espaces accessibles au public », *op.cit.*, p.708.

²⁷⁴ *Ibid.*, p.709.

²⁷⁵ C. DE VALKENEER, *Manuel de l'enquête pénale*, *op.cit.*, p. 515.

²⁷⁶ *Ibid.*

²⁷⁷ C.I.Cr., art. 28ter, § 2, al. 1^{er}.

²⁷⁸ L. BEIRENS, « De politie, uw virtuele vriend? Nadenken over een beleidsmatige aanpak van criminaliteit in virtuele gemeenschappen in cyberspace », *De orde van de dag*, 2010, p.64.

numérique²⁷⁹. La Commission de la protection de la vie privée²⁸⁰ a par ailleurs déjà exprimé la nécessité d'adapter l'article 26 alinéa 2 de la loi sur la fonction de police pour habilitier les fonctionnaires de police à « visiter les espaces virtuels accessibles au public après enregistrement, et pour ainsi dire de faire de la surveillance et des patrouilles sur Internet »²⁸¹. Une telle modification avait d'ailleurs été envisagée²⁸² lors de l'adoption de la loi du 25 décembre 2016²⁸³.

Section III. Recherche dans les sources ouvertes, observation et infiltration

§1. L'article 47sexies du Code d'instruction criminelle

La frontière entre l'exploitation de données publiques qui repose sur l'article 26 de la loi sur la fonction de police et l'observation au sens de l'article 47sexies est également source d'incertitudes²⁸⁴. La question se pose de savoir si la surveillance d'un lieu ou d'une personne sur Internet pourrait être qualifiée d'observation systématique au sens de l'article 47sexies du Code d'instruction criminelle. Cette disposition concerne *a priori* les recherches dans le monde physique mais tout comme l'article 26 de la loi sur la fonction de police, celle-ci pourrait s'appliquer à l'observation virtuelle²⁸⁵.

L'observation systématique est décrite par l'article 47sexies §1^{er} comme l'observation « par un fonctionnaire de police, d'une ou de plusieurs personnes, de leur présence ou de leur comportement, ou de choses, de lieux ou d'événements déterminés ».

L'observation est dite « systématique » lorsqu'elle dure plus de cinq jours consécutifs ou plus de cinq jours non consécutifs répartis sur une période d'un mois, lorsque des moyens techniques sont utilisés, lorsqu'elle revêt un caractère international ou lorsqu'elle est exécutée par des

²⁷⁹ C. FORGET, « La collecte de preuves sur le *darknet* et les espaces accessibles au public », *op.cit.*, p.707.

²⁸⁰ Aujourd'hui Autorité de protection des données.

²⁸¹ C.P.V.P., *Avis n° 13/2015 du 13 mai 2015 sur l'avant-projet de loi portant dispositions diverses – modifications de la loi portant création d'un organe de recours en matière d'habilitations de sécurité, de la loi sur la fonction de police et de la loi du 18 mars 2014 relative à la gestion de l'information policière*, p.6, point 21.

²⁸² Projet de loi relatif à l'amélioration des méthodes particulières de recherche et de certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications, Rapport de G. Calomne et G. uyttersprot fait au nom de la Commission de la justice, *Doc. parl.*, Ch. repr., sess. ord., 2015-2016, n° 54-1966/6, p. 42.

²⁸³ Loi du 25 décembre 2016 portant des modifications diverses au Code d'instruction criminelle et au Code pénal, en vue d'améliorer les méthodes particulières de recherche et certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications et créant une banque de données des empreintes vocales, *M.B.*, 17 janvier 2017, p. 2738.

²⁸⁴ C. FORGET, « La collecte de preuves sur le *darknet* et les espaces accessibles au public », *op.cit.*, p.712.

²⁸⁵ *Ibid.*

unités spécialisées de la police fédérale²⁸⁶. Un moyen technique au sens de cette disposition est « une configuration de composants qui détecte des signaux, les transmet, active leur enregistrement et enregistre les signaux »²⁸⁷, comme par exemple un GPS ou une caméra²⁸⁸. Cette mesure ne peut être mise en œuvre par les services de police qu’après autorisation du procureur du Roi²⁸⁹. Les nécessités de l’enquête doivent justifier le recours à une telle mesure et les autres moyens d’investigation doivent être insuffisants pour arriver à la manifestation de la vérité²⁹⁰. En outre, une observation effectuée à l’aide de moyens techniques n’est possible qu’en présence d’indices sérieux d’infractions de nature à entraîner un emprisonnement correctionnel principal d’un an ou une peine plus lourde²⁹¹.

§2. L’analyse à grande échelle de données publiques : légal ?

Un point important que ni l’arrêt du 28 mars 2017 ni la loi n’aborde est celui « du cadre légal pour l’utilisation d’outils informatiques qui permettent un *monitoring* à grande échelle et systématique de données publiques »²⁹². C’est un point qui intéresse tout particulièrement notre problématique, puisqu’un des défis majeurs pour les autorités répressives qui enquêtent de manière proactive est la capacité à repérer des signes d’exploitation parmi l’ampleur des publications sur Internet, et ainsi permettre une identification rapide des victimes. Nous nous sommes interrogés sur la légalité d’un système qui serait capable de scruter Internet à la recherche d’éventuels signes d’exploitation²⁹³. À titre d’exemple, nous pouvons citer les Pays-Bas, actuellement en train de développer une application numérique (web *crawler*²⁹⁴) pour tenter de détecter des cas d’exploitation sexuelle en ligne²⁹⁵. La situation n’est pas si hypothétique en Belgique quand on sait que la police de Liège s’est doté d’un logiciel permettant de scruter les réseaux sociaux à la recherche d’éventuels troubles à l’ordre public²⁹⁶.

²⁸⁶ C.I.Cr., art. 47*sexies*, § 2.

²⁸⁷ C.I.Cr., Art. 47*sexies*, § 1^{er}, al. 3.

²⁸⁸ M. DE RUE, « La loi du 6 janvier 2003 concernant les méthodes particulières de recherche et quelques autres méthodes d’enquête: premiers commentaires », *Rev. dr. pén.*, 2003/9-10, p. 1109.

²⁸⁹ C.I.Cr., art. 47*sexies*, § 2, al. 1^{er}.

²⁹⁰ C.I.Cr., art. 47*sexies*, § 2, al. 1^{er}.

²⁹¹ C.I.Cr., art. 47*sexies*, § 2, al. 2.

²⁹² K. GEENS, « Défis de la société numérique : perspectives politiques » in *Société numérique et droit pénal Belgique, France, Europe, op.cit.*, p.29.

²⁹³ Voy. B. BREWSTER, T. INGLE and G. RANKIN, « Crawling Open-Source Data for Indicators of Human Trafficking », *2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing*, London, 2014, pp. 714-719.

²⁹⁴ Le web *crawling* est une technique de programme informatique utilisée pour analyser des données accessibles sur des sites web à grande échelle.

²⁹⁵ TWEDE KAMER DER STATEN-GENERAAL, *Brief van de Minister van veiligheid en justitie en Staatssecretaris van Volksgezondheid, welzijn en sport*, vergaderjaar 2019–2020, p.6, disponible sur <https://www.tweedekamer.nl/>.

²⁹⁶ Sud Info, « La police de Liège va scruter les réseaux sociaux avec un logiciel qui analysera tout ce qui est posté: images et commentaires », 7 novembre 2018, disponible sur www.sudinfo.be.

Il nous semble qu'en Belgique la légalité d'un tel système est incertaine. Bien que la Cour de Cassation ait confirmé le fait que les données publiques sont librement exploitables par la police, il faut être prudent quant à la masse de données exploitée et les outils utilisés²⁹⁷. Si la police Belge en venait à se doter d'un logiciel permettant de filtrer un nombre important de données sur des sources ouvertes afin d'y déceler des indicateurs d'exploitation, la question se poserait de savoir si on ne se trouverait pas dans l'hypothèse d'une observation systématique à l'aide de moyens techniques visée par l'article 47sexies §1^{er} alinéa 2 du Code d'instruction criminelle²⁹⁸.

Afin d'exclure, de manière certaine, l'applicabilité de l'article 47sexies à la recherche policière sur les sources publiques, les travaux parlementaires de la loi de 2016 suggéraient de préciser que les observations de sources ouvertes ne requéraient pas d'autorisation au sens de cet article et que l'article 47sexies ne concernait que les observations « non en ligne »²⁹⁹. Une telle modification aurait semble-il été plus conforme à l'article 32 de la Convention sur la cybercriminalité précité³⁰⁰. Reste que celle-ci n'a pas été adoptée et qu'on peut se demander si en matière d'analyse de données à grande échelle, un cadre légal spécifique, respectueux du droit à la vie privée des utilisateurs ne devrait pas être mis en place.

§3. *L'infiltration sur Internet*

Il convient également de préciser que le pouvoir de « patrouiller sur Internet » des autorités policières que nous venons de décrire ne doit pas se confondre avec une mesure d'infiltration sur Internet (dite infiltration « light ») visée par l'article 46sexies du Code d'instruction criminelle. Cette prérogative, calquée sur l'infiltration classique³⁰¹ (47octies C .i .Cr), a été introduite par la loi du 25 décembre 2016. Elle permet aux services de police, sous identité fictive le cas échéant, d'entretenir des contacts sur Internet avec une ou plusieurs personnes concernant lesquelles il existe des indices sérieux qu'elles commettent ou commettraient des infractions pouvant donner lieu à un emprisonnement correctionnel principal d'un an ou à une peine plus lourde. Cette mesure doit être autorisée par le Procureur du Roi. Compte tenu du

²⁹⁷ K. GEENS, *op.cit.*, p.29.

²⁹⁸ C. FORGET, « La collecte de preuves sur le *darknet* et les espaces accessibles au public », *op.cit.*, pp.713- 714.

²⁹⁹ Projet de loi relatif à l'amélioration des méthodes particulières de recherche et de certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications, Rapport de G. Calomne et G. uyttersprot fait au nom de la Commission de la justice, *op.cit.*, p. 42.

³⁰⁰ *Ibid.*

³⁰¹ C. FORGET, « Les nouvelles méthodes d'enquête dans un contexte informatique : vers un encadrement (plus) strict? », *R.D.T.I.*, 2017/1-2, p. 42.

libellé de la disposition (« qu’elles commettent ou commettraient »), il semble que la mesure puisse être utilisée de manière réactive ou proactive³⁰². Les travaux parlementaires soulignent par ailleurs l’utilité de cette mesure en matière de *grooming*³⁰³.

Chapitre II. L’accès au contenu des smartphones des suspects et des victimes

L’analyse des messages, des images et des vidéos à partir de smartphones ou ordinateurs peut apporter des éléments de preuve déterminants dans certains dossiers de traite des êtres humains lorsque ces outils ont été utilisés pour communiquer avec la victime ou pour organiser l’exploitation de la victime. Cette matière est régie par l’article 39 *bis* du Code d’instruction criminelle, qui concerne les recherches non secrètes dans un système informatique.

Section I. La recherche locale (39bis, §2, C.I.Cr.)

L’article 39bis, §2, alinéa 1^{er} du Code d’instruction criminelle régit la recherche de données se trouvant dans un système informatique (smartphone, ordinateur) qui a été saisi³⁰⁴ et qui n’est pas verrouillé³⁰⁵. Celle-ci peut être menée par un officier de police judiciaire³⁰⁶, sans le consentement ou contre le gré de l’utilisateur du système informatique³⁰⁷. La recherche est dite « locale » car elle se limite à l’examen des données sauvegardées sur l’appareil³⁰⁸, et ne peut s’étendre aux données qui sont accessibles *via* ce support informatique mais qui sont stockées ailleurs³⁰⁹. Des informations stockées sur des applications telles que WhatsApp, Facebook, ou Hotmail ne seront pas directement accessibles à moins qu’une partie de ces informations soient stockées sur l’appareil et accessibles hors connexion³¹⁰. Si l’appareil est verrouillé, l’officier de police judiciaire devra au préalable obtenir une autorisation du procureur du Roi³¹¹, qui pourra

³⁰² V. FRANSEN et O. LEROUX, « Recherche policière et judiciaire sur internet : analyse critique du nouveau cadre législatif belge » in *Société numérique et droit pénal Belgique, France, Europe, op.cit.*, p. 193.

³⁰³ Projet de loi relatif à l’amélioration des méthodes particulières de recherche et de certaines mesures d’enquête concernant Internet, les communications électroniques et les télécommunications, Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord., 2015-2016, 54-1966/001, p. 37.

³⁰⁴ C’est-à-dire matériellement soustrait à son propriétaire pour être mis à la disposition de la justice selon l’art. 35 du C.I.Cr.

³⁰⁵ Par un mot de passe, touch ID, face ID, identifiant, etc.

³⁰⁶ C.I.Cr., art. 39bis, §2, al. 1^{er}.

³⁰⁷ V. FRANSEN et O. LEROUX, *op.cit.*, p. 139.

³⁰⁸ L’article 39bis, §2, al. 3 du C.I.Cr. indique que chaque liaison externe du système informatique doit être empêchée avant que la recherche soit entamée. Ceci revient à mettre l’appareil en mode « avion ».

³⁰⁹ L. GRISARD, P. MONVILLE et M. GIACOMETTI, « La collecte des preuves numériques en droit belge après l’arrêt de la Cour constitutionnelle du 5 décembre 2018 », *Rev. dr. pén.*, 2019/9, p. 1008.

³¹⁰ Projet de loi relatif à l’amélioration des méthodes particulières de recherche et de certaines mesures d’enquête concernant Internet, les communications électroniques et les télécommunications, Exposé des motifs, *op.cit.*, p. 17.

³¹¹ C.I.Cr., art. 39bis, §5, al.1^{er}, 1^{er} tiret.

autoriser l'usage de fausses clés pour accéder aux données. Il en va de même si les données stockées dans l'appareil ne sont pas directement accessibles en raison d'un chiffrement, le Procureur du roi pourra autoriser l'usage de dispositifs techniques en vue du décryptage et du décodage des données³¹². Notons qu'une même recherche peut être menée sur un support informatique qui n'a pas été saisi mais qui pourrait l'être³¹³.

En ce qui concerne notre problématique, la recherche locale peut s'avérer utile mais elle est limitée car elle ne permet d'accéder à du contenu en ligne ou à des interactions qui ont eu lieu en ligne. Pour ce faire, il faut étendre la recherche menée dans le système informatique.

Section II. L'extension de recherche (88ter et 39bis, §5, C.I.Cr.)

L'extension de recherche se conçoit comme le prolongement de la mesure de recherche dans un système informatique³¹⁴ et s'apparente à une forme de « perquisition électronique »³¹⁵. L'hypothèse visée ici est celle dans laquelle un support informatique (GSM, ordinateur) a été saisi ou pourrait l'être, et que les enquêteurs souhaitent avoir accès à des données qui ne sont pas directement stockées sur l'appareil mais dans un système informatique distant³¹⁶. Une telle recherche permet notamment d'avoir accès aux réseaux sociaux auxquels le smartphone du suspect est connecté, comme par exemple Facebook³¹⁷.

Le recours à cette mesure relève de la compétence exclusive du juge d'instruction. Notons que la loi du 25 décembre 2016 avait transféré ce pouvoir au parquet, mais que ce glissement de compétence a été condamné par la Cour Constitutionnelle³¹⁸.

La mesure est subordonnée à la réunion de deux conditions. La première exige que la mesure soit nécessaire à la manifestation de la vérité à l'égard de l'infraction qui fait l'objet de la recherche³¹⁹. La seconde implique qu'il doit être recouru à la mesure uniquement si d'autres mesures seraient disproportionnées ou s'il existe un risque que des éléments de preuve soient

³¹² C.I.Cr., art. 39bis, §5, al. 2, 2^e tiret.

³¹³ C.I.Cr., art. 39bis, §2, al. 2.

³¹⁴ M. CORHAY, « L'extension de la recherche dans un système informatique : du droit belge à la Convention de Budapest sur la cybercriminalité », *J.T.*, 2020/8, n° 6804, p. 134.

³¹⁵ B. DOCQUIR, *op.cit.*, p. 610.

³¹⁶ V. FRANSEN et O. LEROUX, *op.cit.*, p. 151.

³¹⁷ Projet de loi relatif à l'amélioration des méthodes particulières de recherche et de certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications, Exposé des motifs, *op.cit.*, p. 18.

³¹⁸ C. const., 6 décembre 2018, n° 174/2018, disponible sur www.const-court.be.

³¹⁹ C.I.Cr., art. 88ter, al. 1^{er}, 1^{er} tiret.

perdus³²⁰. De plus, l'extension de recherche ne peut pas excéder les systèmes informatiques ou les parties de tels systèmes auxquels les personnes autorisées à utiliser le système informatique qui fait l'objet de la mesure ont spécifiquement accès³²¹. Cette dernière restriction entend empêcher une intrusion illimitée dans tous les systèmes susceptibles d'être en relation ou d'être mis en relation avec le système informatique qui fait l'objet de la mesure³²². Ainsi, l'extension de la recherche ne peut s'exercer qu'à l'égard des systèmes présentant une liaison technique, stable permanente et non-occasionnelle avec le système informatique de départ³²³.

Si l'usage d'une fausse clé ou de techniques de décryptage est nécessaire pour accéder aux données distantes, l'intervention du juge d'instruction est également requise³²⁴. Celui-ci peut autoriser, sans le consentement du propriétaire ou de l'utilisateur, la suppression temporaire de toute protection des systèmes informatiques concernés à l'aide de moyens techniques, de faux signaux, de fausses clés ou de fausses qualités, ainsi que l'installation de dispositifs techniques permettant de décrypter et de décoder des données stockées, traitées ou transmises par le système informatique. Pour ce faire, il peut requérir la collaboration de quiconque dont on présume qu'il a une connaissance particulière du système informatique visé relatives à son fonctionnement ou la manière d'y accéder, par exemple les clés de chiffrement ou les mots de passe³²⁵. Il peut s'agir par exemple d'importateurs/de distributeurs d'ordinateurs, de fournisseurs de service, d'opérateurs, d'ingénieurs d'entreprise ayant élaboré une configuration informatique spécifique, de spécialistes de la sécurité³²⁶.

Le paragraphe 7 de l'article 39*bis* indique que : « Sauf si son identité ou son adresse ne peuvent être raisonnablement retrouvées, le procureur du Roi ou le juge d'instruction informe dans les plus brefs délais, le responsable du système informatique de la recherche dans le système informatique ou de son extension. Il lui communique le cas échéant un résumé des données qui ont été copiées, rendues inaccessibles ou retirées ». Il convient de noter que les mesures précitées ne se font pas forcément au départ d'un système informatique appartenant à la personne suspecte, c'est-à-dire dans notre cas de figure le trafiquant. La recherche peut aussi

³²⁰ C.I.Cr., art. 88*ter*, al. 1^{er}, 2^e tiret.

³²¹ C.I.Cr., art. 88*ter*, alinéa 2.

³²² M. CORHAY, *op.cit.*, p. 134 ; Projet de loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord.1999- 2000, n° 0213/001, p. 23.

³²³ *Ibid.*

³²⁴ C.I.Cr., art. 39*bis* §5, al.2.

³²⁵ C.I.Cr., art. 88*quater*, §1^{er}.

³²⁶ Projet de loi relatif à l'amélioration des méthodes particulières de recherche et de certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications, Exposé des motifs, *op.cit.*, p. 50.

s'effectuer au départ du *smartphone* de la victime. En effet, la notion de « responsable du système informatique » ne s'identifie pas à la personne dont les données sont exploitées³²⁷. Or si le suspect n'est pas le responsable du système informatique qui fait l'objet de la recherche et de son extension, celui-ci ne sera pas informé de ladite recherche. Dans ce contexte, la Cour Constitutionnelle a jugé que : « puisque l'obligation d'informer le responsable du système informatique de la recherche est utilisée pour distinguer le caractère secret et non secret d'une investigation et que ceci s'inscrit dans le cadre de la protection des justiciables, il faut considérer que la notification au responsable du système informatique concerne aussi le suspect, dont les données stockées dans le système font l'objet de cette recherche, lorsque le suspect n'exerce pas le contrôle effectif du système informatique concerné »³²⁸.

L'extension de recherche dans un système informatique a potentiellement pour effet de permettre aux autorités belges d'accéder unilatéralement, c'est-à-dire sans passer par l'entraide judiciaire, à des données informatiques stockées sur le territoire d'un autre État³²⁹. Lorsqu'il s'avère que les données ne se trouvent pas sur le territoire du Royaume, elles peuvent seulement être copiées. En ce cas, le juge d'instruction communique sans délai cette information au Service public fédéral Justice, qui en informe les autorités compétentes de l'État concerné, si celui-ci peut raisonnablement être déterminé³³⁰.

Du point de vue du droit international, le principe de territorialité veut que les autorités policières et judiciaires ne soient habilitées à poser des actes que sur le territoire national³³¹. L'article 32, b) de la Convention sur la cybercriminalité constitue une exception à ce principe puisqu'il permet l'accès à des données informatiques stockées dans un autre État sans passer par une procédure d'entraide judiciaire. À ce jour, cet article est réputé « être la seule norme disposant des situations dans lesquelles l'action unilatérale des États est unanimement considérée comme admissible »³³². Notons toutefois que l'article 88ter est rédigé en termes plus larges que ce que prévoit la Convention, ce qui peut potentiellement porter atteinte à la souveraineté des États, un tel élargissement permettant « une immixtion virtuelle sur le territoire d'un État déterminé afin de recueillir des données informatiques »³³³.

³²⁷ L. GRISARD, P. MONVILLE et M. GIACOMETTI, *op.cit.*, p. 1004.

³²⁸ C. const., 6 décembre 2018, point B.15.2.

³²⁹ M. CORHAY, *op.cit.*, p. 137.

³³⁰ C.I.Cr., art. 88ter, al. 4.

³³¹ M. CORHAY, *op.cit.*, p. 137.

³³² *Ibid.*, p.139.

³³³ *Ibid.*

Les mesures précitées peuvent fournir des éléments de preuve importants dans des cas d'exploitation sexuelle. Elles peuvent permettre de prendre connaissance de messages échangés entre le suspect et ses victimes. Elles interviendront généralement à un stade de l'enquête où un suspect aura été interpellé et/ou une ou des victimes potentielles auront été identifiées. En outre elles ne seront possibles qu'en présence d'un système informatique (ordinateur/GSM) à partir duquel mener la recherche.

Chapitre III. La collaboration des fournisseurs de service à l'enquête pénale, un élément essentiel de la lutte contre la traite des êtres humains à l'ère numérique

Section I. L'insuffisance de l'entraide judiciaire internationale

La lutte contre la criminalité dans la société informatique a rendu les autorités policières et judiciaires dépendantes d'entreprises privées qui stockent, traitent ou transmettent des données³³⁴. À l'heure où 80 pourcents de l'infrastructure digitale mondiale est détenue par des entreprises privées³³⁵, l'accès aux données que ces dernières détiennent est indispensable pour mener à bien un nombre significatif d'enquêtes pénales³³⁶. Ce constat est vrai pour toute une série d'infractions laissant des traces digitales³³⁷, ce qui est le cas de l'exploitation sexuelle via Internet.

Lorsque des affaires de traite des êtres humains nécessitent la collecte transfrontière de preuves numériques, les autorités judiciaires peuvent recourir aux mécanismes de l'entraide judiciaire³³⁸. Ces mécanismes permettent, a priori, de remédier à « l'application stricte des principes du droit international au droit de la procédure pénale »³³⁹. Certains instruments existent à cet égard, comme la Convention sur la cybercriminalité, la convention d'entraide judiciaire³⁴⁰ ou la décision d'enquête européenne³⁴¹. L'entraide judiciaire permet à un État requérant de demander à l'État requis l'aide nécessaire pour lui permettre de mener à bien sa

³³⁴ V. FRANSEN et O. LEROUX, *op.cit.*, p. 196.

³³⁵ G. MOUNIER, « Enquêtes internationales et poursuites des cybercriminels – État des lieux des défis juridiques », *Obs. Bxl.*, 2016/3, n°105, p.17.

³³⁶ V. FRANSEN et O. LEROUX, *op.cit.*, p.196.

³³⁷ *Ibid.*, pp. 196-197.

³³⁸ V. FRANSEN, « Droit pénal et numérique : vers un nouveau paradigme », *Rev. Dr. ULiège*, 2018/1, p.203.

³³⁹ A.GOSSÉ., « Dans quelle mesure les autorités judiciaires belges peuvent-elles contraindre des entreprises de télécommunication étrangères à collaborer à une enquête pénale en Belgique ? », *Rev. dr. pén. entr.*, 2017/3, p. 197.

³⁴⁰ Convention européenne d'entraide judiciaire en matière pénale, signée à Strasbourg le 20 avril 1959, approuvée par la loi du 19 juillet 1975, *M.B.*, 23 octobre 1975, p. 13275.

³⁴¹ Directive 2014/41/UE du Parlement européen et du Conseil du 3 avril 2014 concernant la décision d'enquête européenne en matière pénale, *J.O.U.E.*, 1^{er} mai 2014, L 130, p. 1.

mission répressive³⁴². Elle prend la forme d'une commission rogatoire internationale c'est-à-dire un « mandat donné par une autorité judiciaire d'un pays à une autorité judiciaire étrangère à l'effet de procéder en ses lieu et place à un ou plusieurs actes spécifiés par le mandat »³⁴³.

Les mécanismes de l'entraide judiciaire classiques s'avèrent toutefois peu adaptés à l'obtention de preuves numériques³⁴⁴. Trois critiques majeures peuvent leur être adressées : les règles de procédure qu'ils contiennent les rendent lourds d'un point de vue administratif, ils sont lents à mettre en œuvre, et enfin leur efficacité est largement dépendante de la bonne volonté des États requis³⁴⁵. Or la collecte de preuves numériques nécessite des procédures rapides, car ces preuves apparaissent et disparaissent rapidement, et sont soumises aux réglementations relatives à la conservation des données.

Face à ce constat, la coopération internationale directe avec les opérateurs, les fournisseurs d'Internet et autres médias sociaux constitue un défi majeur dans la lutte contre la traite des êtres humains³⁴⁶. Recueillir des preuves relatives à des infractions liées à des cas de traite commises au moyen des technologies de l'information et de la communication nécessite la collaboration d'acteurs privés. Or, les communications ou données liées à ces infractions peuvent s'établir ou être stockées par des fournisseurs officiellement établis à l'étranger. Ceci pose des questions complexes de territorialité dans le monde d'Internet qui par définition ne connaît pas de frontières³⁴⁷. Le rapport de *Myria* de 2017³⁴⁸ indique qu'en Belgique, les autorités collaborent avec des réseaux sociaux comme Facebook dans des dossiers de traite des êtres humains, par une demande d'entraide judiciaire. Le rapport pointe toutefois la lenteur des procédures et le fait que la collaboration dépend largement de la volonté des entreprises privées.

³⁴² M. MARTY, *La légalité de la preuve dans l'espace pénal européen*, Bruxelles, Larcier, 2016, p. 356.

³⁴³ CONSEIL DE L'EUROPE, *Rapport explicatif de la Convention européenne d'entraide judiciaire en matière pénale du 20 avril 1959*, p.5, disponible sur : <https://rm.coe.int/16800c9317#:~:text=La%20Convention%20Europ%C3%A9enne%20d'Entraide%20Judiciaire%2C%20en%20vertu%20d',Europe%20le%2020%20avril%201959.>

³⁴⁴ Voy. not. M. GIACOMETTI, « Collecte transfrontalière de preuves numériques selon le point de vue belge. La décision d'enquête européenne, un moyen approprié ? » in *Société numérique et droit pénal*, op.cit., pp. 287-325 et S. TOSZA, « Cross-border gathering of electronic evidence : mutual legal assistance, its shortcomings and remedies » in *Société numérique et droit pénal*, op.cit., pp. 269-285.

³⁴⁵ A.GOSSÉ, op.cit., p. 197.

³⁴⁶ ASSEMBLÉE INTERPARLEMENTAIRE BENELUX, op.cit., p.19.

³⁴⁷ Projet de loi relatif à l'amélioration des méthodes particulières de recherche et de certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications, Exposé des motifs, op.cit., p. 10.

³⁴⁸ MYRIA, *Rapport annuel traite et trafic des êtres humains*, 2017, op.cit., p.161.

Dans une seconde section nous parcourons les dispositions pertinentes du Code d'instruction criminelle et analysons dans quelle mesure elles permettent une collaboration efficace des autorités répressives et des entreprises privées dans le cadre d'enquêtes de traite des êtres humains à des fins sexuelles.

Section II. Les obligations de collaboration des fournisseurs de services

§1. Mesures susceptibles de nécessiter la collaboration d'entreprises privées

A. L'article 46*bis* : L'identification des personnes publiant des offres à caractère sexuel liées à des faits de traite

Comme l'indique C. de Callatay « contrairement à une idée reçue, personne n'est anonyme sur Internet (...). Lorsqu'un individu consulte une page web, il laisse une trace de son passage sur le site visité, que les hébergeurs de contenu sont en mesure de conserver »³⁴⁹.

Selon l'article 46*bis* du Code d'instruction criminelle le procureur du Roi peut requérir le concours des opérateurs et fournisseurs de communications électroniques afin d'obtenir des informations sur l'utilisateur d'un service. Cet article permet d'obtenir d'une part l'identité et les coordonnées de l'abonné ou de l'utilisateur habituel d'un service de télécommunication³⁵⁰, et d'autre part, les moyens de communication auxquels une personne déterminée est abonnée ou qu'elle utilise de manière habituelle³⁵¹. La disposition visait initialement l'identification de l'utilisateur d'un numéro de téléphone mais a été modifiée en 2007³⁵² pour y introduire la notion de « communication électronique », de sorte que la disposition vise aujourd'hui également les utilisateurs d'Internet³⁵³.

Cet article permet d'obtenir des données personnelles d'un utilisateur du réseau Internet, comme par exemple des documents d'ouverture d'un abonnement à Internet³⁵⁴, la copie de la carte d'identité fournie par le client lors de la conclusion du contrat³⁵⁵ ou encore des coordonnées bancaires liées au règlement de la prestation de service³⁵⁶. L'identification d'un

³⁴⁹ C. DE CALLATAY, *op. cit.*, p. 175.

³⁵⁰ C.I.Cr., art. 46*bis*, §1^{er}, al.1^{er}, 1^{er} tiret.

³⁵¹ C.I.Cr., art. 46*bis*, §1^{er}, al.1^{er}, 2^e tiret.

³⁵² Loi du 23 janvier 2007 modifiant l'article 46*bis* du Code d'instruction criminelle, *M.B.*, 14 mars 2007, p. 13662.

³⁵³ O. LEROUX, « Arnaques, fraudes et escroqueries sur internet : moyens concrets d'investigation – Point sur l'affaire dite *Yahoo!* à la suite du second arrêt de la Cour de cassation », *J.T.*, 2012/40-41, n° 6500, p. 841.

³⁵⁴ *Ibid.*

³⁵⁵ *Ibid.*

³⁵⁶ *Ibid.*

utilisateur du réseau Internet à partir d'un numéro d'adresse IP pourra également être effectuée sur base de l'article 46*bis*, uniquement si cette adresse IP est fixe. L'adresse IP, une suite de chiffres attribuée par le fournisseur d'accès est dite fixe ou dynamique, selon qu'elle reste la même ou varie à chaque connexion³⁵⁷. Le plus souvent, l'adresse IP attribuée par les fournisseurs est dynamique³⁵⁸. Dans ce cas l'identification de l'utilisateur d'Internet ne pourra se faire sur base de l'article 46*bis* que si l'adresse dynamique et le moment de la connexion sont connus. À défaut, il faudra recourir à l'article 88*bis* du Code d'instruction criminelle que nous analysons ci-après. Cette disposition peut également servir de justification pour s'adresser à des fournisseurs de services (hébergement, courrier électronique, commerce en ligne) qui sont susceptibles de détenir des informations sur leurs utilisateurs³⁵⁹.

L'identification d'un utilisateur peut être demandée pour toute infraction³⁶⁰. Elle peut également être demandée dans le cadre d'une recherche proactive³⁶¹. La motivation du recours à la mesure doit refléter le caractère proportionnel eu égard au respect de la vie privée et subsidiaire à tout autre devoir d'enquête³⁶². De plus, pour des infractions qui ne sont pas de nature à entraîner un emprisonnement correctionnel principal d'un an ou une peine plus lourde, le procureur du Roi ne peut requérir les données d'identification que pour une période de six mois préalable à sa décision³⁶³.

C'est sur cette base que des informations sur l'utilisateur qui aurait posté des offres de services sexuels de victimes pourraient être obtenues, en s'adressant aux hébergeurs du contenu relatif à des cas d'exploitation sexuelle.

Le refus des opérateurs ou fournisseurs de service de prêter leur concours technique à l'exécution de la mesure décidée par Procureur du Roi est puni d'une amende de vingt-six à dix mille euros³⁶⁴.

³⁵⁷ C. DE VALKENEER, *Manuel de l'enquête pénale*, op.cit., p.458.

³⁵⁸ A.GOSSÉ, op.cit., p. 182.

³⁵⁹ O. LEROUX, « Arnaques, fraudes et escroqueries sur internet.. », op.cit., p. 840.

³⁶⁰ M. FRANCHIMONT, A. JACOBS et A. MASSET, *Manuel de procédure pénale*, Bruxelles, Larcier, 2012, p. 370.

³⁶¹ *Ibid.*

³⁶² C.I.Cr., art. 46*bis*, §1^{er}, al.3.

³⁶³ C.I.Cr., art. 46*bis*, §1^{er}, al.4.

³⁶⁴ C.I.Cr., art. 46*bis*, §2, al.4.

B. L'article 88bis : Le repérage de communications électroniques ou la localisation de l'origine ou de la destination des communications électroniques entre le trafiquant et la victime

L'article 88bis du Code d'instruction criminelle prévoit la possibilité, pour le juge d'instruction, de faire procéder « au repérage des données de trafic des moyens de communication électronique à partir desquels ou vers lesquels des communications électroniques sont adressées ou ont été adressées »³⁶⁵ ainsi qu'à « la localisation de l'origine ou de la destination de communications électroniques »³⁶⁶. La mesure concerne les communications passées par GSM, mais aussi via une application Internet comme WhatsApp ou Messenger³⁶⁷.

Cette disposition permet l'obtention de données dynamiques qui ne peuvent être isolées à un moment précis dans le temps³⁶⁸. Elle permet par exemple de connaître l'heure, la durée ou encore les correspondants d'une communication électronique³⁶⁹. Ainsi un aperçu des communications et contacts qu'une personne a établis au cours d'une certaine période et la localisation de ces échanges peut être obtenu³⁷⁰. En substance, l'article 88bis permet de savoir qui a communiqué avec qui, quand et où. En revanche, il ne permet pas de connaître le contenu de la communication³⁷¹.

Le recours à l'article 88bis est seulement possible pour les infractions passibles d'une peine d'emprisonnement correctionnel principal d'un an ou d'une peine plus lourde³⁷². En cas de repérages futurs, la mesure ne peut s'étendre au-delà de deux mois, sans préjudice d'un éventuel renouvellement³⁷³. Lorsque la mesure porte sur une période passée, le temps d'accès aux données est fonction de la gravité de l'infraction pour laquelle la mesure est ordonnée³⁷⁴. Cette période est de neuf mois pour les infractions visées à l'article 90ter, §§2 à 4³⁷⁵, ce qui est le cas de la traite des êtres humains (433quinquies C.pén.) , du *grooming* (377quater C.pén.) , et de la cyberprédation (433bis/1 C. pén.).

³⁶⁵ C.I.Cr., art. 88bis, §1^{er}, al.1^{er}, 1^o.

³⁶⁶ C.I.Cr., art. 88bis, §1^{er}, al.1^{er}, 2^o.

³⁶⁷ H. BERKMOES, « Repérage et localisation de télécommunications », in *Postal Mémoires. Lexique du droit pénal et des lois spéciales*, Waterloo, Wolters Kluwer, 2019, p. R 107/24.

³⁶⁸ A.GOSSÉ, *op.cit.*, p. 182.

³⁶⁹ *Ibid.*

³⁷⁰ H. BERKMOES, *op. cit.*, p. 24.

³⁷¹ O. MICHIELS et G. FALQUE, *Principes de procédure pénale*, Bruxelles, Larcier, 2019, p. 258.

³⁷² C.I.Cr., art. 88bis, §1^{er}, al. 1^{er}.

³⁷³ C.I.Cr., art. 88bis, §1, al.5.

³⁷⁴ C. DE VALKENEER, « Chapitre V - L'information et l'instruction » in *La loi pot-pourri II*, Bruxelles, Larcier, 2017, p. 109.

³⁷⁵ C.I.Cr., art. 88bis, §2, 2^e tiret.

Pour mener à bien ses recherches, le juge d'instruction peut solliciter la collaboration d'opérateurs ou de fournisseurs de communications électroniques³⁷⁶. Le refus de ces personnes de prêter leur concours technique à l'exécution des réquisitions du juge d'instruction est puni d'une amende de vingt-six à dix mille euros³⁷⁷.

C. L'article 90ter : La prise de connaissance ou l'interception des communications entre le trafiquant et la victime

L'article 90ter, § 1er, alinéa 1er, du Code d'instruction criminelle permet au juge d'instruction « dans un but secret, d'intercepter, prendre connaissance, explorer et enregistrer, à l'aide de moyens techniques, des communications non accessibles au public ou des données d'un système informatique ou d'une partie de celui-ci, ou étendre la recherche dans un système informatique ou une partie de celui-ci ».

Cette disposition régit tant l'interception de communications que la recherche secrète dans un système informatique, en vue d'enregistrer ou de copier des données contenues dans ce système. Elle permet de prendre connaissance du contenu de communications, en temps réel (interception) ou non, et de manière secrète³⁷⁸ c'est-à-dire « à l'insu des acteurs de ces communications ou à l'insu du propriétaire, du détenteur ou de l'utilisateur du système informatique »³⁷⁹.

Le terme « communications non accessibles au public » vise « des communications relevant de la sphère privée et qui ne sont pas destinées à tout quiconque »³⁸⁰. En ce qui concerne les communications électroniques, la notion vise tout contenu de communications électroniques, il peut s'agir de signes, de messages écrits, de photos, de sons ou encore de vidéos³⁸¹. La disposition se focalise sur le contenu d'une communication qu'elle soit orale ou écrite, analogique ou numérique³⁸². À l'origine, l'article 90ter visait des communications « en cours

³⁷⁶ C.I.Cr., art. 88bis, § 1^{er}, al. 2.

³⁷⁷ C.I.Cr., art. 88bis §4, al.3.

³⁷⁸ V. FRANSSSEN et S. TOSZA, « Vers plus de droits pour le justiciable sur internet ? Un nouveau cadre légal pour lutter contre la criminalité dans la société de l'information », in *Les droits des justiciables face à la justice pénale* (sous la dir. de V. FRANSSSEN et A. MASSET), CUP, vol. 171, Limal, Anthemis, 2017, p. 224.

³⁷⁹ Projet de loi relatif à l'amélioration des méthodes particulières de recherche et de certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications, Exposé des motifs, *op.cit.*, p. 54.

³⁸⁰ *Ibid.*, p. 53.

³⁸¹ M.-A. BEERNAERT, H. D. BOSLY et D. VANDERMEERSCH, *Droit de la procédure pénale*, Bruxelles, la Charte, 2017, tome 1, p. 793.

³⁸² V. FRANSSSEN et S. TOSZA, *op.cit.*, p. 223.

de transmission » mais cette condition a été supprimée car elle n'était pas adaptée aux communications ayant lieu par Internet³⁸³.

Le recours à cette mesure est subordonné à la présence d'indices sérieux quant à l'existence d'infractions limitativement énumérées à l'article 90^{ter} §2 à 5. Cette mesure, de par son caractère intrusif, est uniquement réservée aux faits délictueux les plus graves³⁸⁴. La loi du 25 décembre 2016 a par ailleurs grandement étendu la liste des infractions pour lesquelles cette mesure est envisageable, de sorte que le principe de proportionnalité de cette disposition ne semble être qu'une « garantie de façade »³⁸⁵. Le *grooming* (377^{quater}), le leurre de mineurs par le biais des technologies de l'information et de la communication à des fins criminelles ou délictuelles (433^{bis}/1) et la traite des êtres humains (433^{quinquies} à 433^{octies}) font désormais partie des infractions pour lesquelles des communications peuvent être interceptées³⁸⁶. La mesure est donc applicable à tous les comportements envisagés dans la première partie de ce travail. À cette condition de proportionnalité s'ajoute une condition de subsidiarité. Il ne pourra être recouru à la mesure d'interception que si les autres moyens d'investigation ne suffisent pas à la manifestation de la vérité³⁸⁷. Bien que sensible d'un point de vue du droit à la vie privée, les travaux parlementaires soulignent que le recours à ce type de mesure est loin d'être marginal³⁸⁸.

L'article 90^{ter}, § 1er, al. 4, C.I.Cr. indique que la mesure peut notamment être ordonnée à l'égard des moyens de communications et de télécommunications régulièrement utilisés par un suspect. Ceci vise les hypothèses où un moyen technique de communication ou de télécommunication est utilisé (comme un smartphone ou un ordinateur)³⁸⁹.

³⁸³ Projet de loi relatif à l'amélioration des méthodes particulières de recherche et de certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications, Exposé des motifs, *op.cit.*, p. 54.

³⁸⁴ Selon l'article 21 de la Convention de Budapest, un dispositif d'interception des communications doit être limité aux enquêtes relatives à « un éventail d'infractions graves à définir en droit interne ».

³⁸⁵ L. GRISARD, P. MONVILLE et M. GIACOMETTI, *op.cit.*, p. 1021.

³⁸⁶ L'ajout de ces articles s'inscrivent dans la transposition de la Directive 2011/93/UE du Parlement européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI du Conseil d'une part, et de la directive 2011/36/UE du Parlement européen et du Conseil du 5 avril 2011 concernant la prévention de la traite des êtres humains et la lutte contre ce phénomène ainsi que la protection des victimes et remplaçant la décision-cadre 2002/629/JAI du Conseil d'autre part.

³⁸⁷ C.I.Cr., art. 90^{ter}, § 1er, al. 2.

³⁸⁸ Projet de loi relatif à l'amélioration des méthodes particulières de recherche et de certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications, Rapport de G. Calomne et G. uyttersprot fait au nom de la Commission de la justice, *op.cit.*, p. 58.

³⁸⁹ C. DE VALKENEER, *Manuel de l'enquête pénale*, *op.cit.*, p. 480.

Une mesure basée sur l'article 90^{ter} doit faire l'objet d'une autorisation écrite préalable et motivée du juge d'instruction, que celui-ci communique au procureur du Roi³⁹⁰. Elle ne peut excéder un mois, sans préjudice d'un renouvellement³⁹¹. La durée maximale de la mesure ne peut en aucun cas dépasser six mois³⁹².

En pratique, il arrive souvent que des moyens de communication utilisés par les suspects soient protégés ou chiffrés, et leur contenu par conséquent inaccessible. Tel est notamment le cas d'applications comme WhatsApp, Viber ou encore Skype³⁹³. Ces moyens de communication sont préférés par les trafiquants qui les savent plus difficilement contrôlables par la police³⁹⁴. L'article 90^{ter} §1^{er} alinéa 3 prévoit la possibilité pour le juge d'instruction de supprimer de manière temporaire toute protection des systèmes informatiques concernés à l'aide de moyens techniques, de faux signaux, de fausses clés ou de fausses qualités. De la même manière, il peut décider de l'installation de dispositifs techniques dans les systèmes informatiques concernés en vue du décryptage et du décodage de données stockées, traitées ou transmises par ce système. Pour ce faire, le juge d'instruction peut exiger l'assistance de personnes dont il présume qu'elles ont une connaissance particulière du moyen de communication ou du système informatique qui fait l'objet de la mesure ou de services ou applications qui permettent de protéger, de coder ou de crypter les données qui sont stockées, traitées ou transmises par un moyen de communication ou un système informatique³⁹⁵.

Lorsque la mesure vise des communications sur Internet, la collaboration des opérateurs et/ ou des fournisseurs de service de communication électronique est nécessaire³⁹⁶. Cette collaboration pourra être demandée sur base de l'article 90 *quater* §2 du Code d'instruction criminelle. Les opérateurs et fournisseurs sont tenus de prêter leur concours à l'exécution de la mesure sous peine d'une amende de vingt-six euros à vingt mille euros³⁹⁷.

³⁹⁰ C.I.Cr., art. 90 *quater*, §1^{er}, al. 1^{er}.

³⁹¹ C.I.Cr., art. 90 *quater*, §1^{er}, al. 2, 4^o et art. 90 *quinquies*, al.1^{er}.

³⁹² C.I.Cr., art. 90 *quinquies* al.1^{er}.

³⁹³ C. FORGET, « Les nouvelles méthodes d'enquête dans un contexte informatique : vers un encadrement (plus) strict? », *op.cit.*, p.50.

³⁹⁴ MYRIA, *Rapport annuel traite et trafic des êtres humains*, 2017, *op.cit.*, p.32.

³⁹⁵ C.I.Cr., art. 90 *quater*, §4.

³⁹⁶ A.GOSSÉ, *op.cit.*, p. 184.

³⁹⁷ C.I.Cr., art. 90 *quater*, §2, al. 3.

§2. Champ d'application personnel et territorial des obligations

Les champs d'application personnel et territorial des devoirs de collaboration au sens des articles 46*bis*, 88*bis*, et 90 *quater* du C.I.Cr. ont fait l'objet d'un vif débat en Belgique³⁹⁸, au travers de l'affaire *Yahoo ! Inc* (ci-après *Yahoo*), dans laquelle plusieurs juridictions nationales ont été amenées à se prononcer³⁹⁹ et qui a pris fin par un arrêt de la Cour de Cassation du 1^{er} décembre 2015⁴⁰⁰.

Cette affaire concernait des faits d'escroquerie pour lesquels les suspects avaient utilisé plusieurs adresses e-mail *Yahoo*⁴⁰¹. Ces adresses constituaient la seule trace des suspects. Dans ce contexte, le procureur du Roi de Termonde avait décidé de s'adresser directement à l'entreprise américaine sur base de l'article 46*bis* du Code d'instruction criminelle, afin que celle-ci lui fournisse des données d'identification et autres données ou informations personnelles pouvant mener à l'identification des utilisateurs des adresses e-mail. Yahoo a refusé de collaborer au motif qu'elle n'était ni « un opérateur d'un réseau de communication électronique » ni « un fournisseur d'un service de communication électronique » au sens de l'article 46*bis* du C.I.Cr⁴⁰². En outre, elle soutenait que n'ayant pas de siège social en Belgique, les informations demandées étaient protégées par la législation américaine⁴⁰³ et qu'elles ne pouvaient être obtenues que par la voie d'une commission rogatoire internationale⁴⁰⁴. Cette « saga judiciaire »⁴⁰⁵ qui a opposé le procureur du Roi à l'entreprise Yahoo fut l'occasion pour la Cour de Cassation de préciser le champ d'application d'article 46*bis*, et par la suite ceux des 88*bis* et 90 *quater* §2 du Code d'instruction criminelle.

A. Champ d'application personnel des obligations de collaboration

Dans un arrêt du 18 janvier 2011⁴⁰⁶, la Cour de Cassation a retenu une interprétation large de l'obligation contenue à l'article 46*bis* du C. i. Cr. Elle a précisé que celle-ci : « ne se limite, dès lors, pas aux opérateurs d'un réseau de communications électroniques ou aux fournisseurs d'un

³⁹⁸ V. FRANSSEN et O. LEROUX, *op.cit.*, p. 197.

³⁹⁹ A.GOSSÉ, *op.cit.*, pp. 186-187.

⁴⁰⁰ Cass. (2e ch.), 1er décembre 2015, *Pas.*, 2015/13, p.92.

⁴⁰¹ *Yahoo!* est une société américaine qui propose différents services sur Internet, dont un service de messagerie mail. Son siège social se situe en Californie.

⁴⁰² V. FRANSSEN et O. LEROUX, *op.cit.*, p. 198.

⁴⁰³ En l'espèce, l'« *Electronic Communications Privacy Act* ».

⁴⁰⁴ O. LEROUX, « Arnaques, fraudes et escroqueries sur internet.. », *op. cit.*, p. 841.

⁴⁰⁵ A.GOSSÉ, *op.cit.*, p. 186.

⁴⁰⁶ Cass., 18 janvier 2011, *N.C.*, 2011/1, pp. 76-85.

service de communications électroniques qui sont aussi opérateurs au sens de la loi du 13 juin 2005 ou qui ne dispensent leurs services de communications électroniques qu'au moyen de leur propre infrastructure. Cette obligation existe aussi dans le chef de celui qui fournit un service consistant entièrement ou principalement dans la transmission de signaux par la voie des réseaux de communications électroniques et la personne qui fournit un service consistant à autoriser ses clients à obtenir ou recevoir ou diffuser des informations au moyen d'un réseau électronique peut aussi être un fournisseur d'un service de communications électroniques »⁴⁰⁷.

Cette interprétation extensive est non seulement conforme à la définition de « fournisseurs de service » qui se trouve à l'article 1^{er} de la Convention de Budapest⁴⁰⁸ mais elle permet surtout de viser une série de services web utilisés par beaucoup de criminels : Facebook, Twitter, WhatsApp, Instagram, Gmail, Hotmail. Dans une autre l'affaire, l'affaire *Skype*⁴⁰⁹, un même interprétation large a été validée par la Cour de Cassation en ce qui concerne les obligations contenues aux articles 88*bis* et 90 *quater* §2.

Afin d'éviter de nouvelles controverses quant au champ d'application des obligations de collaboration contenues dans le Code d'instruction criminelle, cette jurisprudence a été codifiée par la loi du 25 décembre 2016. Celle-ci a modifié les articles 46 *bis*⁴¹⁰, 88*bis*⁴¹¹ et 90 *quater* §2⁴¹² pour y inclure la nouvelle définition de fournisseur d'un service de communications électroniques à savoir : « toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations *via* un réseau de communications électroniques. Est également compris le fournisseur d'un service de communications électroniques ». Sont désormais visés les fournisseurs de communications électroniques tels que définis à l'article 2 de la loi du 13 juin 2005 (*sensu stricto*), mais également les autres fournisseurs de services qui rentrent dans la définition légale (*sensu lato*)⁴¹³.

⁴⁰⁷ Cass., 18 janvier 2011, *N.C.*, 2011, p.76, point 6 (ndlr).

⁴⁰⁸ L'article 1^{er}, c) de la Convention vise toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique ainsi que toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs.

⁴⁰⁹ Les faits remontent à septembre 2012 et la Cour de Cassation a mis fin aux discussions par un arrêt du 19 février 2019 ; Cass. (2^e Ch.), 19 février 2019, *Lar. Cass.*, 2020/4, p. 85.

⁴¹⁰ L. 25 décembre 2016, art.5.

⁴¹¹ L. 25 décembre 2016, art.12.

⁴¹² L. 25 décembre 2016, art. 18.

⁴¹³ C. CONINGS et S. ROYER, « Verzamelen en vastleggen van digitaal bewijs in strafzaken » in *Topics bewijs-en procesrecht*, Intersentia, 2017, p. 118.

B. Champ d'application territorial des obligations de collaboration

Vient la question, plus épineuse, du champ d'application territorial des obligations de collaboration. En effet, la plupart des services Internet que nous utilisons quotidiennement, qui sont aussi utilisés par les criminels sont offerts par des fournisseurs établis à l'étranger (le plus souvent aux États-Unis mais aussi ailleurs). Considérer que ces prestataires doivent se soumettre aux législations nationales de tous les pays où ils sont virtuellement présents peut sembler juridiquement extrêmement contraignant, à l'inverse estimer que ces prestataires ne devraient se soumettre qu'aux législations du pays où se situe leur siège social ou leurs serveurs n'est pas non plus satisfaisant⁴¹⁴.

Dans l'affaire *Yahoo*, la Cour de Cassation a jugé que tout fournisseur de communications électroniques qui offre un service sur le territoire belge est soumis aux obligations de collaboration, au même titre qu'un opérateur de téléphonie comme Proximus⁴¹⁵. Cette précision quant au champ d'application territorial ressort désormais expressément des dispositions du Code d'instruction criminelle telles que modifiées par la loi du 25 décembre 2016⁴¹⁶. Ceci implique que le procureur du Roi (pour l'article 46*bis*) ou un juge d'instruction (pour les articles 88*bis* et 90 *quater* §2) peut ordonner directement à Google, Facebook, WhatsApp, Skype, ainsi qu'à tous ceux qui rentrent dans la définition légale de collaborer à des poursuites pénales ouvertes en Belgique⁴¹⁷. Précisons qu'en ce qui concerne les données d'identification (article 46*bis*) l'approche belge est en totale conformité avec la Convention de Budapest⁴¹⁸ qui, en son article 18. 1 b) donne la possibilité aux États parties d'adopter des mesures législatives afin d'ordonner à un fournisseur de services offrant des prestations sur son territoire de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services.

⁴¹⁴ A. GOSSÉ, *op.cit.*, p. 190.

⁴¹⁵ K. GEENS et de S. BIOLLEY, « L'accès aux données de communication par Internet dans les enquêtes pénales. Les efforts belges pour aboutir à une législation UE ambitieuse et novatrice » in *L'Europe au présent !*, Bruxelles, Bruylant, 2018, p. 463.

⁴¹⁶ Les art 46*bis* §1^{er}, 88*bis* §1^{er} et 90 *quater* §2 visent « toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service ... ».

⁴¹⁷ K. GEENS et de S. BIOLLEY, *op.cit.*, p. 464.

⁴¹⁸ V. FRANSSEN et M. CORHAY « La fin de la saga Skype : les fournisseurs de services étrangers obligés de collaborer avec la justice belge en dépit des possibilités techniques et de leurs obligations en droit étranger », *R.D.C.-T.B.H.*, 2019/8, p. 1016.

Ces évolutions récentes sont importantes en terme de moyens pour contrer l'utilisation d'Internet dans le cadre de la traite des êtres humains. Premièrement, les mesures précitées sont toutes potentiellement applicables à l'infraction de traite des êtres humains et aux infractions connexes qui l'entourent (*grooming*, cyberprédation). Deuxièmement, la totalité des plateformes qui sont utilisées par les trafiquants, que cela soit pour recruter les victimes ou vendre leurs services, entrent désormais sans difficulté dans la définition de « fournisseur de service de communications électroniques » (champ d'application personnel). Enfin ces plateformes ont l'obligation de collaborer même si elles sont hébergées à l'étranger, ou si le siège social de leur société est à l'étranger (champ d'application territorial). Il en résulte que dans le cadre de poursuites, les autorités peuvent obtenir des plateformes de précieuses informations sur l'identité d'un suspect et sur les échanges entretenus avec la victime.

Si ces obligations de collaboration constituent « une arme solide pour les autorités judiciaires belges »⁴¹⁹ qui semble indispensable pour lutter contre la criminalité dans le monde informatique, cette approche unilatérale adoptée par la Belgique se heurte à la fois à la souveraineté des États et aux droits fondamentaux des utilisateurs de services⁴²⁰. L'affaire *Skype* est une illustration des problèmes que peuvent engendrer une telle approche⁴²¹. Dans cette affaire *Skype* avait refusé de répondre aux obligations contenues aux articles 88*bis* §2 et 90 *quater* §2 du C.I.Cr, notamment car cette collaboration avec la justice belge l'aurait obligé à violer les règles luxembourgeoises relatives à la confidentialité des communications privées⁴²². La Cour de Cassation a tout simplement refusé l'argument du conflit de loi, au motif que les communications ciblées par les demandes du juge d'instruction se situaient en Belgique et non au Luxembourg⁴²³. Cette jurisprudence, favorable aux autorités belges, met les opérateurs et fournisseurs de services étrangers actifs sur le marché belge « dans une situation inextricable: soit ils respectent leur obligation de collaboration en droit belge, soit ils violent la législation de l'État de leur siège social »⁴²⁴.

La Belgique n'est pourtant pas la seule à recourir à ce type de solution de manière unilatérale. D'autres pays délaissent les mécanismes classiques de l'entraide judiciaire pour leur préférer la

⁴¹⁹ A.GOSSÉ, *op.cit.*, p. 191.

⁴²⁰ V. FRANSSSEN et O. LEROUX, *op.cit.*, p. 203.

⁴²¹ *Ibid.*

⁴²² V. FRANSSSEN et M. CORHAY, *op.cit.*, p. 1016.

⁴²³ *Ibid.*, p.1020.

⁴²⁴ *Ibid.*, 1021.

collaboration directe avec des entreprises privées⁴²⁵, et ce en raison de l'utilisation répandue d'Internet pour communiquer et échanger de l'information. En la matière il semble toutefois qu'une réglementation européenne ou internationale serait préférable⁴²⁶ afin de fixer un cadre juridique clair et d'éviter des difficultés de collaboration comme celles survenues dans les affaires *Yahoo* ou *Skype*.

Deux projets en cours méritent d'être soulignés à cet égard. La proposition *e-evidence* de la Commission européenne, qui contient en réalité deux instruments, une directive⁴²⁷ et un règlement⁴²⁸, souhaite créer un cadre juridique efficace pour permettre aux autorités répressives et judiciaires d'obtenir plus facilement et plus rapidement les preuves électroniques dont elles ont besoin pour mener à bien leurs enquêtes. Elle prévoit des règles pour permettre aux autorités judiciaires de s'adresser directement à un fournisseur de service dans un État membre, tout en insistant sur la protection des droits fondamentaux de la personne dont les données sont exploitées. Mieux réglementer la coopération directe en vue de l'obtention de preuves numériques est également une préoccupation du Conseil de l'Europe. En effet c'est l'un des objectifs du futur second Protocole à la Convention sur la cybercriminalité⁴²⁹.

⁴²⁵ *Ibid.*, p. 1020.

⁴²⁶ *Ibid.* p. 1019.

⁴²⁷ Proposition de directive du Parlement européen et du Conseil établissant des règles harmonisées concernant la désignation de représentants légaux aux fins de la collecte de preuves en matière pénale, COM/2018/226 final – 2018/0107 (COD), disponible sur : <https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52018PC0226&from=EN>.

⁴²⁸ Proposition de Règlement du Parlement européen et du Conseil relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale, COM/2018/225 final – 2018/0108(COD), disponible sur : https://eur-lex.europa.eu/resource.html?uri=cellar:639c80c9-4322-11e8-a9f4-01aa75ed71a1.0002.02/DOC_1&format=PDF

⁴²⁹ COMITÉ DE LA CONVENTION SUR LA CYBERCRIMINALITÉ, Mandat pour la préparation d'un projet de 2e protocole à la convention sur la cybercriminalité, Strasbourg, 9 juin 2017, disponible sur : <https://rm.coe.int/mandat-pour-la-preparation-d-un-projet-de-2e-protocole-a-la-convention/168072380f>.

Conclusion

Ce travail avait pour but d'analyser dans quelle mesure le droit pénal et le droit de la procédure pénale répondent efficacement à l'usage grandissant des technologies de l'information et de la communication, plus particulièrement d'Internet, dans le cadre de la traite sexuelle.

Au terme de notre analyse nous constatons tout d'abord que tous les comportements relatifs à l'usage d'Internet dans le cadre de la traite sexuelle que nous avons identifiés tombent sous le coup de l'application de dispositions pénales. Que ce soit le recrutement des victimes sur Internet, qui peut relever selon les cas des articles relatifs à la traite, au *grooming* ou à la cyberprédation, ou la publicité de services sexuels qui tombe sous l'application de l'article 380^{ter} du Code pénal. Les incriminations relatives au recrutement peuvent potentiellement intervenir à un stade précoce, lorsque que la victime n'a pas encore été exploitée. Toutefois le recrutement des victimes par Internet rend cette étape de la traite moins visible de sorte qu'il peut être difficile pour les autorités répressives de repérer ces comportements de manière autonome, avant la phase d'exploitation. À ce stade, Internet crée un effet « boîte noire ». Nous constatons également que bien que les plateformes mettant en avant des annonces à caractère sexuel pourraient être poursuivies pour ce type d'activité, la Belgique se montre tolérante envers ce phénomène, notamment parce que les sites de ce type peuvent servir à l'identification de victimes. L'usage d'Internet à ce stade a pour effet, contrairement au recrutement, de rendre les victimes plus visibles. Nous soulignons, par ailleurs, la certaine contradiction dans laquelle se placent les autorités répressives belges en collaborant avec des sites qui sont ouvertement illégaux. Cela résulte, à notre sens, d'une politique répressive de la prostitution qui manque de cohérence, mais cela dépasse la contribution de ce travail.

Pour ce qui est des réponses à apporter à l'usage d'Internet par les trafiquants, il apparaît que notre problématique s'inscrit dans un mouvement plus général d'adaptation du droit de la procédure pénale pour lutter contre la criminalité dans le monde numérique. Nous remarquons que l'arsenal législatif belge est plutôt complet en ce qui concerne la collecte de la preuve sur Internet, et donc apte à répondre à l'usage grandissant d'Internet pour faciliter la traite sexuelle. Nous pensons par ailleurs que le cadre législatif existant en matière de recherches sur les sources publiques d'Internet doit être précisé afin d'autoriser les services de police à faire de la surveillance continue sur Internet, à la recherche d'éventuels signes d'exploitation et de

potentielles victimes. Un cadre légal adapté est nécessaire mais pas suffisant, car combattre et punir les activités illégales sur Internet demande des moyens techniques adaptés.

En ce qui concerne la collaboration des acteurs privés à l'enquête pénale, la problématique à laquelle nous nous sommes intéressés prend place dans un contexte où une vraie gouvernance d'Internet reste à construire, dans un monde où la lutte contre toutes sortes de criminalités doit s'effectuer dans le monde physique comme dans le monde virtuel. On peut tout de même déjà se réjouir du fait que le Code d'instruction criminelle belge permette aux autorités de s'adresser directement aux fournisseurs de services qui peuvent détenir des éléments de preuve importants dans des cas de traite sexuelle via Internet.

Nous terminerons par souligner qu'un cadre légal adapté pour répondre à la problématique de la traite sexuelle via Internet doit se développer dans le respect des droits fondamentaux de chacun. En effet, toutes les mesures que nous avons mentionnées peuvent potentiellement porter atteinte à la vie privée des utilisateurs d'Internet. Nous pensons que la préservation des droits fondamentaux des victimes de traite sexuelle ne saurait se faire au détriment des droits fondamentaux des autres utilisateurs du cyberspace. Les travaux en cours au niveau européen et international devraient permettre d'assurer cet équilibre.

Bibliographie

1. Législation

1.1 Internationale

- Protocole additionnel à la Convention des Nations Unies contre la criminalité transnationale organisée visant à prévenir, réprimer et punir la traite des personnes, en particulier des femmes et des enfants, fait à New York le 15 novembre 2000, signé à Palerme le 12 décembre 2002, approuvé par la loi du 24 juin 2004, *M.B.*, 13 octobre 2004, p.71306.
- Convention des Nations Unies contre la criminalité transnationale organisée faite à New York le 15 novembre 2000, signée à Palerme le 12 décembre 2002, approuvée par la loi du 24 juin 2004, *M.B.*, 13 octobre 2004, p.71306.
- Convention du Conseil de l'Europe sur la lutte contre la traite des êtres humains, signée à Varsovie le 16 mai 2005, approuvée par la loi du 3 juin 2007, *M.B.*, 27 juillet 2009, p.50141.
- Convention des Nations Unies pour la répression de la traite des êtres humains et de l'exploitation de la prostitution d'autrui, approuvée par l'Assemblée générale dans sa résolution 317 (IV) du 2 décembre 1949, approuvée par la loi du 6 mai 1965, *M.B.*, 13 août 1965, p.9581.
- Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels, , signée à Lanzarote le 25 octobre 2007, approuvée par la loi du 7 février 2012, *M.B.*, 21 juin 2013, p. 39977.
- Convention sur la cybercriminalité, signée à Budapest le 23 novembre 2001, approuvée par la loi du 3 août 2012, *M.B.*, 21 novembre 2012, p.69092.
- Convention européenne d'entraide judiciaire en matière pénale, signée à Strasbourg le 20 avril 1959, approuvée par la loi du 19 juillet 1975, *M.B.*, 23 octobre 1975, p. 13275.

1.2 Européenne

- Action commune du 24 février 1997 adoptée par le Conseil sur la base de l'article K.3 du traité sur l'Union européenne, relative à la lutte contre la traite des êtres humains et l'exploitation sexuelle des enfants, *J.O.U.E.*, 4 mars 1997, L 63, p. 2.
- Décision-cadre 2002/629/JAI du Conseil du 19 juillet 2002 relative à la lutte contre la traite des êtres humains, *J.O.U.E.*, 1er août 2002, L 203, p. 1.
- Directive 2011/36/UE du Parlement européen et du Conseil du 5 avril 2011 concernant la prévention de la traite des êtres humains et la lutte contre ce phénomène ainsi que la protection des victimes et remplaçant la décision-cadre 2002/629/JAI du Conseil, *J.O.U.E.*, 15 avril 2011, L 101, p. 1.
- Directive 2011/92/UE du Parlement européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI du Conseil, *J.O.U.E.*, 17 décembre 2011, L 335, p.1.
- Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur, *J.O.C.E.*, 17 juillet 2000, L 178, p. 1.
- Directive 2014/41/UE du Parlement européen et du Conseil du 3 avril 2014 concernant la décision d'enquête européenne en matière pénale, *J.O.U.E.*, 1^{er} mai 2014, L 130, p. 1.

- Proposition de directive du Parlement européen et du Conseil établissant des règles harmonisées concernant la désignation de représentants légaux aux fins de la collecte de preuves en matière pénale, COM/2018/226 final – 2018/0107 (COD).
- Proposition de Règlement du Parlement européen et du Conseil relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale, COM/2018/225 final – 2018/0108(COD).

1.3. Belge

1.3.1 Codes

- C. pén., art. 65, 322, 324, 377*quater*, 379, 380, 380*ter*, 383*bis*, 433*bis*/1, 433*quinquies*.
- C.I.Cr., art. 28*bis*, 28*ter*, 35, 39*bis*, 46*bis*, 46*sexies*, 47*sexies*, 88*bis*, 88*ter*, 88*quater*, 90*ter*, 90 *quater*.
- C.D.E., art. XII. 19 et 20.

1.3.2 Lois

- Loi du 25 juin 2004 portant assentiment aux actes internationaux suivants : 1° la Convention des Nations unies contre la criminalité transnationale organisée; (...) ; 3° le Protocole additionnel la Convention des Nations unies contre la criminalité transnationale organisée visant à prévenir, réprimer et punir la traite des personnes, en particulier des femmes et des enfants, faits à New York le 15 novembre 2000; (...) , *M.B.*, 13 octobre 2004, p. 701306.
- Loi du 29 avril 2013 visant à modifier l'article 433 *quinquies* du Code pénal en vue de clarifier et d'étendre la définition de la traite des êtres humains, *M.B.*, 23 juillet 2013, p. 45880.
- Loi du 21 août 1948 supprimant la réglementation officielle de la prostitution, *M.B.*, 13 septembre 1948, p. 7352.
- Loi du 13 juin 2005 relative aux communications électroniques, *M.B.*, 20 juin 2005, p.28070.
- Loi du 22 mai 2019 relative au trafic d'organes humains et relative au principe de non-sanction des victimes de traite des êtres humains, *M.B.*, 21 juin 2019, p. 63970.
- Loi du 10 avril 2014 relative à la protection des mineurs contre la sollicitation à des fins de perpétration d'infractions à caractère sexuel, *M.B.*, 30 avril 2014, p.35484.
- Loi du 10 avril 2014 modifiant le Code pénal en vue de protéger les enfants contre les cyberprédateurs, *M.B.*, 30 avril 2014, p. 35486.
- Loi du 27 mars 1995 insérant un article 380*quinquies* dans le Code pénal et abrogeant l'article 380*quater*, alinéa 2, du même Code, *M.B.*, 25 avril 1995, p.10822.
- Loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information, *M.B.*, 17 mars 2003, p.12963.
- Loi du 15 décembre 2013 portant insertion du Livre XII, « Droit de l'économie électronique» dans le Code de droit économique, *M.B.*, 14 janvier 2014, p.1524.
- Loi du 5 août 1992 sur la fonction de police, *M.B.*, 22 décembre 1992, p.27124.
- Loi du 23 janvier 2007 modifiant l'article 46*bis* du Code d'instruction criminelle, *M.B.*, 14 mars 2007, p. 13662.

- Loi du 25 décembre 2016 portant des modifications diverses au Code d'instruction criminelle et au Code pénal, en vue d'améliorer les méthodes particulières de recherche et certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications et créant une banque de données des empreintes vocales, *M.B.*, 17 janvier 2017, p.2738.

1.3.3. Travaux parlementaires

- Projet de loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord.1999- 2000, n° 0213/001.
- Projet de loi visant à modifier l'article 433**quinquies** du Code pénal afin d'étendre la définition de la traite des êtres humains à l'exploitation sexuelle, Amendement n° 1 de Mme Van Cauter, *Doc. parl.*, Ch. repr., sess. ord. 2012-2013, n° 53-2607/2.
- Projet de loi visant à modifier l'article 433**quinquies** du Code pénal afin d'étendre la définition de la traite des êtres humains à l'exploitation sexuelle, Rapport fait au nom de la Commission de la Justice, *Doc. parl.*, Ch. Repr., sess. ord. 2012- 2013, n° 53-2607/4.
- Proposition de loi incriminant le commerce d'organes et le tourisme de transplantation, Rapport fait au nom de la commission de la santé publique, de l'environnement et du renouveau de la société, *Doc. parl.*, Ch. repr., sess. ord. 2018-2019, n° 54-3537/004.
- Projet de loi modifiant diverses dispositions en vue de renforcer la lutte contre la traite et le trafic des êtres humains, Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord., 2004-2005, n° 1560/001.
- Proposition de loi modifiant le Code pénal en vue de protéger les enfants contre les cyberprédateurs, Rapport fait au nom de la commission de la justice, *Doc. Parl.*, Ch. repr., sess. ord. 2013-2014, n° 53-3450/002.
- Proposition de loi modifiant le Code pénal en vue de garantir la protection pénale des enfants contre le « grooming » (mise en confiance à des fins d'abus sexuel), Développements, *Doc. parl.*, Sén., sess. ord. 2012-2013, n° 5-1823/1.
- Projet de loi insérant un article 380 **quinquies** dans le code pénal et abrogeant l'article 380 **quater**, deuxième alinéa, du même Code, Rapport fait au nom de la commission de la justice, *Doc. parl.*, Sén., sess. ord. 1994-1995, n° 1246/2.
- Projet de loi relatif à la protection pénale des mineurs, Exposé des motifs, *Doc. Parl.*, Ch. repr., sess. ord. 1998-1999, n°1907/1.
- Projet de loi relatif à l'amélioration des méthodes particulières de recherche et de certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications, Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord., 2015-2016, 54-1966/001.
- Projet de loi relatif à l'amélioration des méthodes particulières de recherche et de certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications, Rapport de G. Calomne et G. uyttersprot fait au nom de la Commission de la justice, *Doc. parl.*, Ch. repr., sess. ord., 2015-2016, n° 54-1966/6.

1.3.4. Autres

- Circulaire du 23 décembre 2016 relative à la mise en œuvre d'une coopération multidisciplinaire concernant les victimes de la traite des êtres humains et/ou certaines formes aggravées de trafic des êtres humains, *M.B.*, 10 mars 2017, p. 35370.

1.4. Législation étrangère

- Telecommunications Act of 1996, Pub. L. No. 104-104, tit. V (1996).
- Stop Enabling Sex Traffickers Act (SESTA).
- Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA).

2. Jurisprudence

2.1. Européenne

- C.J.U.E., 23 mars 2010 (Google France et Google c. Louis Vuitton Malletier), Aff. jointes C-236/08 à C-238/08, EU:C:2010:159.
- C.J.U.E., 12 juillet 2011 (L'Oréal SA et autres contre eBay International AG et autres), EU:C:2011:474.
- C.J.U.E., 16 février 2012 (SABAM c. Netlog), C-360/10, EU:C:2012:85:1036.

2.2. Belge

- C. const., 6 décembre 2018, n° 174/2018, disponible sur www.const-court.be.
- Cass., 3 janvier 1962, *Pas.*, 1962, I, p. 514.
- Cass., 20 novembre 2001, *Pas.*, 2001, II, p.1906.
- Cass., (2^e ch.), 3 février 2004, *Pas.*, 2004, I, p. 200.
- Cass., 18 janvier 2011, *N.C.*, 2011/1, p. 76.
- Cass., 8 octobre 2014, *Rev. dr. pén. crim.*, 2015, p. 692.
- Cass. (2^e ch.), 1^{er} décembre 2015, *Pas.*, 2015/13, p.92.
- Cass. (2^e ch.), 28 mars 2017, *Pas.*, 2017/3, p. 759.
- Cass., 5 juin 2018, *R.W.*, 2018-2019/9, p. 346.
- Corr. Liège (8^e ch.), 11 février 2009, *Rev.dr.pén.crim.*, p. 963.
- Corr. Liège (19^e ch.), 23 novembre 2016, disponible sur : https://www.myria.be/files/h16-11-16_Corr_Li+%C2%BFge.pdf.
- Corr. Gand, 28 juin 2018, disponible sur : https://www.myria.be/files/h18-06-29_corr_Gent.pdf.
- Liège, 1^{er} juin 2017, disponible sur : https://www.myria.be/files/h17-06-01_a_Li%C3%A8ge.pdf.

3. Doctrine

3.1. Monographies

- BEELEN A., CHARLIER C. et VIGNERON J., *Guide pratique des plateformes*, Bruxelles, Larcier, 2021.
- BEERNAERT M.-A., BOSLY H. D. et VANDERMEERSCH D., *Droit de la procédure pénale*, Bruxelles, la Charte, 2017, tome 1.
- C.-E. CLESSE, *La traite des êtres humains - Droit belge éclairé des législations française, luxembourgeoise et suisse*, Bruxelles, Larcier, 2013.
- CLESSE C.-E., KURZ F., LE COCQ P., et TRUILLET V., *La traite des êtres humains et le travail forcé*, Bruxelles, Éditions Larcier, 2014.
- DE NAUW A. et KUTY F., *Manuel de droit pénal spécial*, Liège, Wolters Kluwer, 2018.
- DE NAUW A., *Initiation au droit pénal spécial*, Waterloo, Kluwer, 2008.
- DE VALKENEER C., *Manuel de l'enquête pénale*, Bruxelles, Editions Larcier, 2018.
- DECHAMPS F. et LAMBILOT C., *Cybercriminalité - État des lieux*, Limal, Anthémis, 2016.
- DOCQUIR B., *Droit du numérique*, Bruxelles, Éditions Larcier, 2018.
- FRANCHIMONT M., JACOBS A. et MASSET A., *Manuel de procédure pénale*, Bruxelles, Éditions Larcier, 2012.
- HENROTTE J.-F. et JONGEN F., *Pas de droit sans technologie*, Bruxelles, Éditions Larcier, 2015.
- JONGEN F. et STROWEL A., *Droit des médias et de la communication*, Bruxelles, Éditions Larcier, 2017.
- LAGASSE F. et PALUMBO M., *Manuel de droit pénal social*, Bruxelles, Éditions Larcier, 2011.
- MARTY M., *La légalité de la preuve dans l'espace pénal européen*, Bruxelles, Éditions Larcier, 2016.
- MICHIELS O. et FALQUE G., *Principes de procédure pénale*, Bruxelles, Éditions Larcier, 2019.
- PLOUFFE-MALETTE K., *Protection des victimes de traite des êtres humains*, Bruxelles, Bruylant, 2013.

3.2. Contributions à un ouvrage collectif

- BERKMOES H., « Repérage et localisation de télécommunications », in *Postal Memorialis. Lexique du droit pénal et des lois spéciales*, Waterloo, Wolters Kluwer, 2019, pp. R 107/1-107/36.
- BRIÈRE C. et WEYEMBERGH A., « L'Union européenne et la traite des êtres humains », in *Fondements et objectifs des incriminations et des peines en droit européen et international* (sous la dir. de D. BERNARD, Y. CARTUYVELS, C. GUILLAIN, D. SCALIA et M. VAN DE KERCHOVE), Limal, Anthémis, 2013, pp. 67-93.
- CLESSE C.-E., « Les organisations internationales et la traite des êtres humains », in *Fondements et objectifs des incriminations et des peines en droit européen et international* (sous la dir. de D. BERNARD, Y. CARTUYVELS, C. GUILLAIN, D. SCALIA et M. VAN DE KERCHOVE), Limal, Anthémis, 2013, pp. 95-110.

- CLESSE C.-E., « Chapitre XI - La traite des êtres humains » in *Les infractions – Volume 2 – Les infractions contre les personnes* (sous la coord. de BOSLY H.D. et DE VALKENEER C.), Bruxelles, Larcier, 2020, pp. 751-825.
- CONINGS C. et ROYER S., « Verzamelen en vastleggen van digitaal bewijs in strafzaken » in *Topics bewijs- en procesrecht*, Intersentia, 2017.
- D. CHICHOYAN, « Traite des êtres humains » in *Droit pénal et procédure pénale*, Malines, Wolters Kluwer, 2014, pp. 99-122.
- DE VALKENEER C., « Chapitre V - L'information et l'instruction » in *La loi pot-pourri II*, Bruxelles, Éditions Larcier, 2017, pp. 91-131.
- FESLER D. et DEHARENG E., « La responsabilité des hébergeurs et des intermédiaires au regard du développement des services en ligne » in *Le droit des nouvelles technologies et de l'internet*, Bruxelles, Bruylant, 2012, pp. 63-98.
- FORGET C., « Chapitre 6 - Méthodes d'enquête pénales et protection des personnes vulnérables dans l'environnement numérique » in *Vulnérabilités et droits dans l'environnement numérique* (sous la coord. de JACQUEMIN H. et NIHOUL M.), Bruxelles, Éditions Larcier, 2018, pp. 179-203.
- FRANSSEN V. et LEROUX O., « Recherche policière et judiciaire sur internet : analyse critique du nouveau cadre législatif belge » in *Société numérique et droit pénal Belgique, France, Europe* (sous la dir. de V. FRANSSEN et D. FLORE), Bruxelles, Bruylant, 2019, pp. 133-215.
- FRANSSEN V. et TOSZA S., « Vers plus de droits pour le justiciable sur internet ? Un nouveau cadre légal pour lutter contre la criminalité dans la société de l'information », in *Les droits des justiciables face à la justice pénale* (sous la dir. de FRANSSEN V. et MASSET A.), CUP, vol. 171, Limal, Anthemis, 2017, pp. 205-249.
- GEENS K. et de BIOLLEY S., « L'accès aux données de communication par Internet dans les enquêtes pénales. Les efforts belges pour aboutir à une législation UE ambitieuse et novatrice » in *L'Europe au présent !*, Bruxelles, Bruylant, 2018, pp. 457-476.
- GEENS K., « Défis de la société numérique : perspectives politiques » in *Société numérique et droit pénal Belgique, France, Europe* (sous la dir. de V. FRANSSEN et D. FLORE), Bruxelles, Bruylant, 2019, pp. 21-34.
- GIACOMETTI M. et MONVILLE P., « 6 - Réseaux sociaux, anonymat et faux profils : vrais problèmes en droit pénal et de la procédure pénale », in *Les réseaux sociaux et le droit* (sous la dir. de SALMON M.), Bruxelles, Éditions Larcier, 2014, pp. 179-210.
- GIACOMETTI M., « Collecte transfrontalière de preuves numériques selon le point de vue belge. La décision d'enquête européenne, un moyen approprié ? » in *Société numérique et droit pénal Belgique, France, Europe* (sous la dir. de V. FRANSSEN et D. FLORE), Bruxelles, Bruylant, 2019, p. 287-325.
- HENRION T., « Protection pénale des mineurs » in *Droit pénal et procédure pénale*, Malines Wolters Kluwer, 2017, pp. 41-160.
- LEONARD T., « 4 - Les réseaux sociaux face à l'exonération de responsabilité des intermédiaires de l'internet : une application délicate » in *Les réseaux sociaux et le droit* (sous la dir. de SALMON M.), Bruxelles, Éditions Larcier, 2014, pp. 123-150.
- LEROUX O., « Section 2. - Criminalité informatique aspécifique » in *Les infractions – Volume 1*, Bruxelles, Éditions Larcier, 2016, pp. 509-534.
- MASSET A., « Protection des mineurs en ligne en droit pénal belge » in *Société numérique et droit pénal Belgique, France, Europe* (sous la dir. de V. FRANSSEN et D. FLORE), Bruxelles, Bruylant, 2019, pp. 47-72.

- MATHIEU G. et. RASSON A.-C, « Chapitre 11 - Les droits de l'enfant dans l'environnement numérique : à la recherche d'un subtil équilibre entre protection et autonomie » in *Vulnérabilités et droits dans l'environnement numérique* (sous la coord. de JACQUEMIN H. et NIHOUL M.), Bruxelles, Éditions Larcier, 2018, pp. 395-464.
- MATHIEU G., « Chapitre 16. - Les droits de l'enfant et Internet : entre autonomie et protection » in *L'Europe des droits de l'homme à l'heure d'Internet* (sous la dir. de VAN ENIS Q. et DE TERWANGNE C.), Bruxelles, Bruylant, 2019, pp. 581-618.
- MONVILLE P. et HOLZAPFEL D., « La prostitution, le droit pénal dans une drôle de posture... », in *Omniprésence du droit pénal. Nouvelles approches pluridisciplinaires* (sous la dir. de RADELET N.), Limal, Anthemis, 2017, pp. 13-28.
- NAGELS C. et LEMONNE A., « Titre IX - Traiter la traite : quand la prostituée navigue dans les eaux troubles de la dignité humaine » in *Sexe et normes*, Bruxelles, Bruylant, 2012, pp. 227-252.
- TOSZA S., « Cross-border gathering of electronic evidence : mutual legal assistance, its shortcomings and remedies » in *Société numérique et droit pénal Belgique, France, Europe* (sous la dir. de FRANSSSEN V. et FLORE D.), Bruxelles, Bruylant, 2019, pp. 269-285.
- TURGIS S., « Chapitre 3. - Les droits de l'homme à l'heure d'Internet et du numérique : rupture ou continuité ? » in *L'Europe des droits de l'homme à l'heure d'Internet* (sous la dir. de VAN ENIS Q. et DE TERWANGNE C.), Bruxelles, Bruylant, 2019, pp. 93-128.

3.3. Articles de périodique

- ALGOET I. « La traite des êtres humains : une nouvelle Hydre de Lerne ? Discours de rentrée prononcé à l'occasion de la rentrée de la cour du travail de Mons, le 4 septembre 2017 », *Rev. dr. pén. entr.*, 2018/1, pp. 3-17.
- ANDRÉ S., « Ceci n'est pas de l'abolitionnisme. Le régime juridique de la prostitution : un surréalisme à la belge ? », *Rev. Dr. ULiège*, 2017/3, pp. 473-493.
- BEERNAERT M.-A. et LE COCQ P. « La loi du 10 août 2005 modifiant diverses dispositions en vue de renforcer la lutte contre la traite et le trafic des êtres humains et contre les pratiques des marchands de sommeil. », *Rev. dr. pén.*, 2006/4, pp. 335-406.
- BEIRENS L., « De politie, uw virtuele vriend? Nadenken over een beleidsmatige aanpak van criminaliteit in virtuele gemeenschappen in cyberspace », *De orde van de dag*, 2010, pp. 51-68.
- BREWSTER B., INGLE T. and RANKIN G., « Crawling Open-Source Data for Indicators of Human Trafficking », *2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing*, London, 2014, pp. 714-719.
- C.-E. CLESSE, « Le recrutement : une action active ou passive ? », note sous Cass., 8 octobre 2014, *Rev. dr. pén. crim.*, 2015, pp. 695-701.
- CHARPENEL Y., « L'exploitation de la prostitution, une affaire d'argent. », *Rev. dr. pén.*, 2013/9-10, pp. 844-853.
- CONINGS C. et VAN LINTHOUT P., « Sociale media – Een nieuwe uitdaging voor politie en justitie », *Panopticon*, 2012, vol. 3, pp. 205-230.
- CORHAY M., « L'extension de la recherche dans un système informatique : du droit belge à la Convention de Budapest sur la cybercriminalité », *J.T.*, 2020/8, n° 6804, pp. 133-141.
- DE CALLATAÏ C., « Les responsabilités liées aux messages postés sur internet : l'extension du régime d'exonération de responsabilité des intermédiaires aux acteurs du web 2.0 », *A&M*, 2013/3-4, pp. 166-182.

- DE RUE M., « La loi du 6 janvier 2003 concernant les méthodes particulières de recherche et quelques autres méthodes d'enquête: premiers commentaires », *Rev. dr. pén.*, 2003/9-10, pp. 1107-1141.
- DESAIVE D., « La coexistence des préventions visées aux articles 433quinquies, § 1, 1°, et 380, alinéa 1, 1° et 4°, du Code pénal », *Rev. dr. pén.* 2010, liv. 7-8, pp. 966-972.
- DIERICKX A., « Noopt nieuwe seksuele criminaliteit tot nieuwe seksuele misdrijven ? », *N.C.*, 2017/3, pp. 207-239.
- DONOVAN E. M., « Fight Online Sex Trafficking Act and Stop Enabling Sex Traffickers Act: A Shield for Jane Doe », *Connecticut Law Review*, 2020, pp. 85-122.
- FORGET C., « La collecte de preuves sur le *darknet* et les espaces accessibles au public », note sous Cass., 28 mars 2017, *Rev. Dr. Pén. Crim.*, pp. 705-715.
- FORGET C., « Les nouvelles méthodes d'enquête dans un contexte informatique : vers un encadrement (plus) strict? », *R.D.T.I.*, 2017/1-2, n° 66-67, pp. 25-52.
- FRANSSEN V. et CORHAY M. « La fin de la saga *Skype* : les fournisseurs de services étrangers obligés de collaborer avec la justice belge en dépit des possibilités techniques et de leurs obligations en droit étranger », *R.D.C.-T.B.H.*, 2019/8, pp. 1014-1022.
- FRANSSEN V., « Droit pénal et numérique : vers un nouveau paradigme », *Rev. Dr. ULiège*, 2018/1, pp. 195-203.
- GOSSÉ A., « Dans quelle mesure les autorités judiciaires belges peuvent-elles contraindre des entreprises de télécommunication étrangères à collaborer à une enquête pénale en Belgique ? », *Rev. dr. pén. entr.*, 2017/3, pp. 179-204.
- GRISARD L., MONVILLE P. et GIACOMETTI M., « La collecte des preuves numériques en droit belge après l'arrêt de la Cour constitutionnelle du 5 décembre 2018 », *Rev. dr. pén.*, 2019/9, pp. 993-1032.
- HARDOUIN R., « La connaissance de l'illicéité par les hébergeurs ou quand être notifié ne signifie pas nécessairement devoir retirer », *R.D.T.I.*, 2012/2, n° 47, pp. 5-19.
- HUBERTS C. et MINET J.-F., « La loi du 29 avril 2013 visant à modifier l'article 433quinquies du code pénal en vue de clarifier et d'étendre la définition de la traite des êtres humains: analyse et mise en perspective. », *Rev. dr. pén.*, 2014/1, pp. 6-48.
- HUBERTS C., « Les innovations de la loi du 10 août 2005 modifiant diverses dispositions en vue de renforcer la lutte contre la traite des êtres humains et le trafic des êtres humains et contre les pratiques des marchands de sommeil », *J.D.J.*, 2006, pp. 6-22.
- JACQUEMIN H., « Responsabilité et numérique : le régime d'exonération de responsabilité des prestataires intermédiaires », *For. Ass.*, 2018/9, n° 188, pp. 177-182.
- KHALAILEH Y. and KISSWANI N. (2015) 'Using technology in human trafficking: international law perspective and reflections within Middle Eastern countries', *Int. J. Technology Policy and Law*, Vol. 2, No. 1, pp. 27-54.
- KURZ F., « Un trop long dimanche de fiançailles ou lorsque le respect de la tradition mène au viol et à la traite des êtres humains », *J.D.J.*, 2014/9, n° 339, pp. 23-29.
- LEROUX O., « Arnaques, fraudes et escroqueries sur internet : moyens concrets d'investigation – Point sur l'affaire dite *Yahoo!* à la suite du second arrêt de la Cour de cassation », *J.T.*, 2012/40-41, n° 6500, pp. 839-843.
- LEROUX O., « La corruption de la jeunesse et les outrages publics aux bonnes mœurs par courrier électronique (courriel, SMS, MMS) », *R.D.T.I.*, n° 17/2003, pp. 13-24.
- LEVI L., « Vers la pénalisation du client dans la lutte contre la prostitution forcée ? », *Rev. dr. pén.*, 2020/11, pp. 1021-1047.
- MASSET A., « Regard actualisé d'un pénaliste sur la prostitution », *R.F.D.L.*, 2015/1, pp. 81-97.

- MCKNELLY M., « Untangling SESTA/FOSTA: How the Internet's 'Knowledge' Threatens Anti-Sex Trafficking Law », *Berkeley Technology Law Journal*, 2019, pp. 1239-1266.
- MINET J.-F., « L'évaluation de la politique belge en matière de lutte contre la traite des êtres humains : le rapport du GRETA », *Rev. dr. pén. entr.*, 2013/4, pp. 105-109.
- MONTERO E., DEMOULIN M. et LAZARO CH., « La loi du 11 mars 2003 sur les services de la société de l'information », *J.T.*, 2004, pp. 81-95.
- MOUNIER G., « Enquêtes internationales et poursuites des cybercriminels – État des lieux des défis juridiques », *Obs. Bxl.*, 2016/3, n°105, pp. 14-18.
- NEDERLANDT O., « Protection des victimes de traite des êtres humains – Approches internationales et européennes », *J.T.*, 2015/6, n° 6592, pp. 157-158.
- PRYLINSKI K.M., « Tech Trafficking: How the internet has transformed sex trafficking », *Journal of High Technology Law*, 2020, pp. 338-372.
- RAETS S. et JANSSENS J., Trafficking and Technology: Exploring the Role of Digital Communication Technologies in the Belgian Human Trafficking Business, *European Journal on Criminal Policy and Research*, 2019, pp. 1-24.
- STEVENS L., « Grooming en cyberlokkend strafbaar. Uitbreiding van de strafrechtelijke bescherming van de seksuele integriteit van minderjarigen in cyberspace », *R.W.*, 2014-2015/22, pp. 844-855.
- TRIPP H., « All sex workers deserve protection: How fosta/sesta overlooks consensual sex workers in an attempt to protect sex trafficking victims », *Penn State Law Review*, 2019, pp. 219-246.
- VERMEULEN G., « Een stille seksuele strafrechtsrevolutie. Verrassende realiteitszin inzake seksueel strafrecht in het nieuwe Strafwetboek », *Panopticon*, 2018/6, pp. 479-488.

3.3. Autres : Études, avis, rapports

- ASSEMBLÉE INTERPARLEMENTAIRE BENELUX, Session 2019, Séances plénières des 14 et 15 juin 2019, compte rendu analytique des réunions, *Débat thématique sur la Traite des êtres humains et les technologies innovantes en vue de lutter contre la traite des êtres humains*.
- C.P.V.P., *Avis n° 13/2015 du 13 mai 2015 sur l'avant-projet de loi portant dispositions diverses – modifications de la loi portant création d'un organe de recours en matière d'habilitations de sécurité, de la loi sur la fonction de police et de la loi du 18 mars 2014 relative à la gestion de l'information policière*.
- COMITÉ DE LA CONVENTION SUR LA CYBERCRIMINALITÉ, Mandat pour la préparation d'un projet de 2e protocole à la convention sur la cybercriminalité, Strasbourg, 9 juin 2017, disponible sur <https://rm.coe.int/mandat-pour-la-preparation-d-un-projet-de-2e-protocole-a-la-convention/168072380f>.
- COMMISSION EUROPÉENNE, Deuxième rapport sur les progrès réalisés dans la lutte contre la traite des êtres humains (2018) établi conformément à l'article 20 de la directive 2011/36/UE concernant la prévention de la traite des êtres humains et la lutte contre ce phénomène ainsi que la protection des victimes, 2018, p. 4, disponible sur : <https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52018DC0777&from=FR>.
- CONSEIL DE L'EUROPE, *Rapport explicatif de la Convention du Conseil de l'Europe sur la lutte contre la traite des êtres humains*, disponible sur <https://rm.coe.int/16800d388d>.
- CONSEIL DE L'EUROPE, *Rapport explicatif de la Convention européenne d'entraide judiciaire en matière pénale du 20 avril 1959*, disponible sur : <https://rm.coe.int/16800c9317#:~:text=La%20Convention%20Europ%C3%A9enne%20d'>

Entraide%20Judiciaire%2C%20en%20vertu%20d'Europe%20le%2020%20avril%201959.

- CONSEIL DE L'EUROPE, *Traite des êtres humains : recrutement par internet*, 2007, disponible sur <https://rm.coe.int/16806eeec1>.
- DEMARÉE C. et VERHOFSTADT C. pour Child Focus, « Les victimes de proxénètes d'adolescents à Bruxelles - Étude exploratoire sur l'existence de la problématique et sa prise en charge possible à Bruxelles », juin 2020, disponible sur https://childfocus.be/sites/default/files/child_focus-tienerpooiers-fr.pdf.
- EUROPOL, *Trafficking in human beings in the EU*, Situation report, La Haye, février 2016, disponible sur : <https://www.europol.europa.eu/publications-documents/trafficking-in-human-beings-in-eu>.
- Facebook's Anti-Slavery and Human Trafficking Statement, [https://s21.q4cdn.com/399680738/files/doc_downloads/2020/06/2020-Facebook's-Anti-Slavery-and-Human-Trafficking-Statement-\(FINAL\).pdf](https://s21.q4cdn.com/399680738/files/doc_downloads/2020/06/2020-Facebook's-Anti-Slavery-and-Human-Trafficking-Statement-(FINAL).pdf).
- FONDATION SCELLES, 5^e Rapport mondial, *Système prostitutionnel - Nouveaux défis, nouvelles réponses*, 2019, disponible sur : <https://www.fondationscelles.org/>.
- GRETA, *Rapport concernant la mise en œuvre de la Convention du Conseil de l'Europe sur la lutte contre la traite des êtres humains par la Belgique*, 2017, p.46, disponible sur : <https://rm.coe.int/2nd-rd-rpt-bel/1680766bdb>.
- MYRIA, *Rapport annuel traite et trafic des êtres humains*, 2010, disponible sur <https://www.myria.be/files/Traite-rapport-2010.pdf>.
- MYRIA, *Rapport annuel traite et trafic des êtres humains*, 2017, disponible sur : <https://www.myria.be/files/RA-TEH-17.pdf>.
- N. PASSAS et al., *Guides législatifs pour l'application de la Convention des Nations unies contre la criminalité transnationale organisée et des Protocoles s'y rapportant*, 1^{ere} partie, New York, Publications des Nations Unies, 2004.
- PARLEMENT EUROPÉEN, *Réforme du régime européen de responsabilité des intermédiaires en ligne – Contexte de la future législation relative aux services numériques*, mai 2020, disponible sur [https://www.europarl.europa.eu/RegData/etudes/IDAN/2020/649404/EPRS_IDA\(2020\)649404_FR.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2020/649404/EPRS_IDA(2020)649404_FR.pdf).
- SERVICE DE LA POLITIQUE CRIMINELLE, *Rapport bisannuel du Gouvernement relatif à la lutte contre la traite des êtres humains 2007-2008*, p. 18, disponible sur <http://www.dsb-spc.be/doc/pdf/RapportTEH2007-2008fr.pdf>.
- SURF AND SOUND, *Improving and sharing knowledge on the Internet role in the processes of human trafficking and smuggling*, 2017, p.98, disponible sur <http://www.surfandsound.eu/>.
- TRACE, *Report on the role of current and emerging technologies in human trafficking*, 2015, pp.79-80, disponible sur https://humantraffickingsearch.org/wp-content/uploads/2017/07/TRACE_D4.1_Role-of-technologies-in-human-trafficking_FINAL.-1.pdf.
- TWEDE KAMER DER STATEN-GENERAAL, *Brief van de Minister van veiligheid en justitie en Staatssecretaris van Volksgezondheid, welzijn en sport, vergaderjaar 2019–2020*, disponible sur <https://www.tweedekamer.nl/>.

4. Articles de presse

- RTL Info, « Le site de petites annonces Vivastreet.be, plateforme de prostitution ? Le fondateur se défend », 31 mai 2018, disponible sur www.rtl.be.
- Le Figaro, « Vivastreet poursuivi pour “proxénétisme aggravé” », 31 mai 2018, disponible sur www.lefigaro.fr.
- Sud Info, « La police de Liège va scruter les réseaux sociaux avec un logiciel qui analysera tout ce qui est posté: images et commentaires », 7 novembre 2018, disponible sur www.sudinfo.be.

