

Faculté de droit et de criminologie

Anonymat et pseudonymat sur les réseaux sociaux : quelles sont les procédures permettant de révéler l'identité des auteurs d'infractions ?

Auteur : Clara Beyaert

Promoteur : Bernard Mouffe

Année académique 2022-2023

Master en droit à finalité droit européen

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

Je tiens à remercier toutes les personnes qui m'ont aidée lors de la rédaction de ce mémoire.

Tout d'abord, je souhaite remercier mon promoteur, Monsieur BERNARD MOUFFE, pour son accompagnement, sa disponibilité ainsi que ses conseils, qui m'ont aidée à réaliser ce mémoire.

Je remercie également Monsieur OLIVIER BOGAERT, membre de la *Federal Computer Crime Unit*, de m'avoir accordé son temps afin de répondre à mes questions, me permettant ainsi de comprendre les enjeux pratiques de ma question de recherche.

Enfin, j'aimerais remercier mes proches pour leur soutien tout au long de mes études et particulièrement pour leur aide et leur relecture de ce mémoire. Une attention particulière pour mon grand-père, qui m'a inspirée, encouragée et aidée tout au long de mes années d'université.

Table des matières

INTRODUCTION	1
PARTIE 1 : GÉNÉRALITÉS	3
CHAPITRE 1 : DÉFINITION DE CONCEPTS-CLÉS	3
<i>Section 1 : Anonymat et pseudonymat</i>	<i>3</i>
<i>Section 2 : Réseaux sociaux</i>	<i>6</i>
CHAPITRE 2 : LIBERTÉS FONDAMENTALES EN TENSION SUR LES RÉSEAUX SOCIAUX.....	8
<i>Section 1 : Droit à la liberté d'expression.....</i>	<i>8</i>
<i>Section 2 : Droit à la vie privée</i>	<i>13</i>
<i>Section 3 : Équilibre entre le droit à la liberté d'expression et le droit à la vie privée sur les réseaux sociaux</i>	<i>16</i>
PARTIE 2 : PROCÉDURES D'IDENTIFICATION DES AUTEURS D'INFRACTIONS SUR LES RÉSEAUX SOCIAUX.....	19
CHAPITRE 1 : RÉGIME D'AUTORÉGULATION DES RÉSEAUX SOCIAUX	21
<i>Section 1 : Champ d'application</i>	<i>22</i>
<i>Section 2 : Point de vue critique</i>	<i>24</i>
CHAPITRE 2 : OBLIGATION D'INFORMATION DES PRESTATAIRES DE SERVICES DE LA SOCIÉTÉ DE L'INFORMATION (DIRECTIVE 2000/31/CE).....	25
<i>Section 1 : Base juridique</i>	<i>25</i>
<i>Section 2 : Champ d'application</i>	<i>26</i>
<i>Section 3 : Principe de non-responsabilité pour les actes des utilisateurs</i>	<i>30</i>
<i>Section 4 : Point de vue critique</i>	<i>32</i>
<i>Section 5 : Digital Services Act (DSA).....</i>	<i>33</i>
CHAPITRE 3 : OBLIGATION DE COLLABORATION DE L'OPÉRATEUR D'UN RÉSEAU DE COMMUNICATION OU D'UN FOURNISSEUR DE SERVICES DE COMMUNICATION ÉLECTRONIQUE (ARTICLE 46BIS DU CODE D'INSTRUCTION CRIMINEL).....	35
<i>Section 1 : Base juridique</i>	<i>35</i>
<i>Section 2 : Champ d'application</i>	<i>36</i>
<i>Section 4 : Point de vue critique</i>	<i>41</i>
CHAPITRE 4 : INJONCTION DANS LE CADRE D'UNE ILLÉGALITÉ EN MATIÈRE DE DROITS DE LA PROPRIÉTÉ INTELLECTUELLE (DIRECTIVE 2001/29/CE ET DIRECTIVE 2004/48/CE).....	43
<i>Section 1 : Base juridique</i>	<i>43</i>
<i>Section 2 : Champ d'application</i>	<i>44</i>
<i>Section 3 : Jurisprudence de la Cour de justice de l'Union européenne</i>	<i>44</i>
<i>Section 4 : Point de vue critique</i>	<i>49</i>

PARTIE 3 : PROCÉDURES D'OBTENTION DES PREUVES NUMÉRIQUES	51
CHAPITRE 1 : COLLECTE TRANSFRONTALIÈRE DE PREUVES NUMÉRIQUES (DIRECTIVE 2014/41/UE)	52
Section 1 : Base juridique	52
Section 2 : Champ d'application	53
Section 3 : Point de vue critique	54
CHAPITRE 2 : INJONCTIONS EUROPÉENNES DE PRODUCTION ET DE CONSERVATION DES PREUVES ÉLECTRONIQUES EN MATIÈRE PÉNALE (RÈGLEMENT 2023/1543 ET DIRECTIVE 2023/1544)	55
Section 1 : Règlement (UE) 2023/1543 du 12 juillet 2023 relatif aux injonctions européennes de production et de conservation concernant les preuves électroniques dans le cadre des procédures pénales et aux fins de l'exécution de peines privatives de liberté prononcées à l'issue d'une procédure pénale	55
Section 2 : Directive (UE) 2023/1544 du 12 juillet 2023 établissant des règles harmonisées concernant la désignation d'établissements désignés et de représentants légaux aux fins de l'obtention de preuves électroniques dans le cadre des procédures pénales	57
CHAPITRE 3 : ENTRAIDE JUDICIAIRE INTERNATIONALE DANS LA COLLECTE DE PREUVES NUMÉRIQUES (CONVENTION SUR LA CYBERCRIMINALITÉ DU CONSEIL DE L'EUROPE)	58
Section 1 : Base juridique	58
Section 2 : Champ d'application	58
Section 3 : Point de vue critique	60
Section 4 : Deuxième Protocole additionnel relatif au renforcement de la coopération et de la divulgation de preuves électroniques du 12 mai 2022	61
CONCLUSION	63
ANNEXE : ENTRETIEN AVEC MONSIEUR OLIVIER BOGAERT, MEMBRE DE LA FEDERAL COMPUTER CRIME UNIT (FCCU), LE 31 JUILLET 2023	65
BIBLIOGRAPHIE	71
LÉGISLATION	71
JURISPRUDENCE	74
DOCTRINE	75
SOURCES INTERNET	81
DIVERS	82

Introduction

Près de 87,7% des personnes âgées de 18 ans et plus sont actives sur les réseaux sociaux¹. Offrant une multitude de possibilités d'interactions en ligne, les réseaux sociaux sont devenus une part essentielle du quotidien de beaucoup d'entre nous. Pour certains, les réseaux sociaux permettent de garder le contact avec la famille ou les amis d'enfance, pour d'autres ils représentent une source de divertissement, un outil professionnel ou commercial, etc.

Si certains choisissent de communiquer leur véritable identité, d'autres préfèrent se présenter sous un pseudonyme. Des associations de défense des libertés individuelles, telles que l'*Electronic Frontier Foundation* et *Human Rights Watch*, ont plaidé en faveur de la possibilité d'utiliser un pseudonyme sur les réseaux sociaux. Leur principal argument était que l'anonymat permettait de garantir « la sécurité, le respect de la vie privée, la confidentialité et la dignité »² des utilisateurs. La doctrine identifie un autre avantage, à savoir celui de désinhiber les mœurs : « Dans le monde virtuel, il y a beaucoup moins d'interdits que dans le monde réel. »³ On peut de la sorte débattre sur des sujets sensibles sans avoir peur des réactions des autres utilisateurs.

L'anonymat et le pseudonymat sont des choix personnels qui n'intéressent pas le droit en tant que tel⁴. Les individus sont libres de créer un compte sur un réseau social et de le gérer comme ils l'entendent, dans le respect des conditions générales d'utilisation. En revanche, en cas d'abus, le droit doit permettre à la justice d'intervenir pour réprimer ces comportements. Par exemple, le cyberharcèlement, touchant un adolescent sur trois en Belgique⁵, est devenu une préoccupation majeure dans nos sociétés. L'anonymat sur les plateformes permettrait aux harceleurs de se livrer à des propos blessants et agressifs en se sentant protégés derrière une identité factice. Cela crée un déséquilibre de forces entre la victime, dont l'identité est connue, et ses harceleurs, dont l'identité est cachée. Malheureusement, le cyberharcèlement n'est qu'un exemple d'infractions impliquant un auteur anonyme sur les réseaux sociaux. On peut

¹X. DEGRAUX, « Réseaux sociaux en Belgique : toutes les statistiques 2023 (étude) », disponible sur <https://www.xavierdegraux.be/reseaux-sociaux-belgique-statistiques-2023-etude>, consulté le 5 juin 2023.

²*Ibid.*

³M. GIACOMETTI et P. MONVILLE, « 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 M. SALMON), Bruxelles, Larcier, 2014, p. 181.

⁴*Ibid.*

⁵Amnesty International Belgique Jeunes, « Le cyberharcèlement, on en parle ? », disponible sur <https://jeunes.amnesty.be/jeunes/informe/notre-blog/article/cyberharcèlement>, consulté le 3 mai 2022.

également évoquer les infractions de faux en informatique, de piratage ou hacking, ainsi que les atteintes aux droits de la propriété intellectuelle. Vu l'augmentation de ces infractions, il est légitime de se demander quelle est la réponse du droit. Quelles sont les procédures qui existent afin de révéler l'identité de l'auteur d'infractions sur les réseaux sociaux ? Peut-on envisager un droit donné à la victime de demander la levée de l'anonymat des auteurs ? Ces questions soulèvent des enjeux importants dans notre société numérique en constante évolution.

Partant de cette problématique, le mémoire se structurera de la manière suivante :

La première partie de ce mémoire examinera les généralités, en définissant, dans son premier chapitre, des concepts-clés tels que l'anonymat/pseudonymat et les réseaux sociaux. Dans le deuxième chapitre, la tension entre le droit à la liberté d'expression et le droit à la vie privée sera abordée, ainsi que leur application sur les réseaux sociaux.

La deuxième partie se concentrera sur les procédures permettant d'identifier un auteur anonyme. Nous commencerons par analyser, au premier chapitre, le régime d'autorégulation des plateformes. Le deuxième chapitre examinera l'obligation d'information pesant sur les prestataires de la société de l'information et le régime de responsabilité de ces derniers en vertu de la Directive 2000/31/CE et révisé par le Règlement (UE) 2022/2065 (DSA). Dans le troisième chapitre, nous aborderons l'obligation de collaboration des plateformes prévue à l'article 46bis du Code d'instruction criminelle. Le dernier chapitre de cette partie se sera consacré à la procédure d'injonction faite aux fournisseurs d'accès à internet pour les infractions liées aux droits de propriété intellectuelle prévue par les Directives 2001/29/CE et 2004/48/CE.

Enfin, la troisième partie abordera les procédures d'obtention de preuves numériques. Nous analyserons au premier chapitre la collecte transfrontalière de preuves numériques mise en place par la Directive 2014/41/UE. Dans le deuxième chapitre, nous nous pencherons sur la nouvelle procédure d'injonctions européennes de production et de conservation des preuves électroniques en matière pénale, qui vient d'être mise en place par le Règlement 2023/1543 et la Directive 2023/1544. Enfin, le dernier chapitre traitera de la coopération judiciaire internationale prévue par la Convention sur la cybercriminalité de Budapest et son deuxième Protocole additionnel relatif au renforcement de la coopération et de la divulgation de preuves électroniques.

Partie 1 : Généralités

Chapitre 1 : Définition de concepts-clés

Section 1 : Anonymat et pseudonymat

Sous-section 1 : Anonymat

La notion d'anonymat peut être complexe à appréhender. D'une part, l'anonymat peut être perçu comme un manque de valeur ou d'existence intrinsèque, voire comme une menace⁶. D'autre part, il peut être considéré comme une stratégie de protection, de préservation, porteuse d'égalité⁷.

La question se pose ici de savoir comment l'anonymat se trouve préservé sur internet et plus spécifiquement sur les réseaux sociaux.

Plusieurs moyens techniques permettent actuellement de garantir un certain degré d'anonymat, tels que l'utilisation d'un anonymiseur pour consulter des pages web, l'utilisation de logiciels « *peer to peer* » pour masquer l'adresse IP, l'utilisation d'un VPN, la connexion à un réseau anonyme via l'installation d'un logiciel, l'intrusion sur le réseau d'un particulier ou encore la complicité d'un fournisseur d'accès. Ces illustrations mettent en évidence le niveau de technicité requise pour garantir un anonymat complet sur internet. Cela nécessite des compétences informatiques avancées et il n'est sans doute pas donné à tout un chacun de pouvoir utiliser ces types de logiciels. L'usage de ces techniques informatiques conduirait à un anonymat absolu.

Toutefois, il existe d'autres degrés d'anonymat sur internet. C'est ce qu'affirme la Cour européenne des droits de l'homme (ci-après « Cour eur. D.H. ») dans son l'arrêt Delfi⁸. Elle indique qu'un internaute peut être anonyme pour le grand public tout en étant identifiable par un prestataire de services, grâce à un compte ou des coordonnées qui peuvent faire l'objet de vérifications plus ou moins poussées, allant d'une vérification limitée à l'authentification

⁶ M. UNTERSINGER, *Anonymat sur internet : comprendre pour protéger sa vie privée*, 1^e édition, Paris, Eyrolles, 2013, p. 1.

⁷*Ibid.*

⁸Cour eur. D.H., arrêt Delfi AS c. Estonie, 16 juin 2015, n°64569/09.

sécurisée, « telle que l'utilisation d'une carte nationale d'identité électronique ou de données d'authentification bancaire en ligne pour identifier un internaute »⁹. En effet, « si un individu crée un compte sur le réseau social Facebook et qu'il ne met aucune information personnelle, ce dernier sera anonyme pour les autres utilisateurs mais pas pour le fournisseur d'accès qui aura l'information qu'il s'est connecté sur Facebook »¹⁰. L'anonymat est, à ce moment-là, non pas absolu mais relatif¹¹.

Dans la suite de l'arrêt, la Cour évalue les implications de l'anonymat sur internet, et considère tout d'abord que l'anonymat est favorable à l'exercice de la liberté d'expression¹². Cependant, elle reconnaît également que l'anonymat facilite la diffusion de propos injurieux et d'actes illicites qui peuvent nuire aux autres utilisateurs¹³. Il s'agit là de l'ambivalence de l'anonymat¹⁴. Comparé aux médias traditionnels, internet facilite certes la communication de l'information, toutefois ses contenus peuvent parfois porter atteinte à autrui, d'autant plus qu'ils peuvent rester indéfiniment accessibles¹⁵. En plus du caractère persistant, la Cour prend notamment en compte la rapidité et l'ampleur de la diffusion des informations sur internet¹⁶.

Sous-section 2 : Pseudonymat

L'obtention d'un anonymat absolu est possible mais difficile à atteindre en pratique sur les réseaux sociaux ; il est plus approprié de parler d'anonymat relatif, étroitement lié au concept de pseudonymat.

Le Règlement général sur la protection des données (ci-après « RGPD ») de l'Union européenne traite spécifiquement de la notion de pseudonymisation en son article 4. Selon cette disposition, il s'agit de données à caractère personnel qui ont été modifiées de manière à ne plus pouvoir être attribuées à une personne physique identifiée ou identifiable, sans avoir recours à

⁹Cour eur. D.H., arrêt Delfi AS c. Estonie, 16 juin 2015, n°64569/09, §148.

¹⁰M. UNTERSINGER, *op. cit.*, p. 2.

¹¹*Ibid.*

¹²Cour eur. D.H., arrêt Delfi AS c. Estonie, 16 juin 2015, n°64569/09, §98.

¹³Cour eur. D.H., arrêt Delfi AS c. Estonie, 16 juin 2015, n°64569/09, §147.

¹⁴N. DE BACKER, « Le principe de proportionnalité à l'épreuve de la liberté d'expression numérique », *J.E.D.H.*, 2019/4, pp. 256-257.

¹⁵Cour eur. D.H., arrêt Delfi AS c. Estonie, 10 octobre 2013, n°64569/09, §92.

¹⁶Cour eur. D.H., arrêt Delfi AS c. Estonie, 10 octobre 2013, n° 64569/09, §147.

des informations supplémentaires¹⁷. Par ailleurs, le pseudonymat correspond au choix de l'identité sous laquelle une personne s'exprime en fonction du lieu et du contexte¹⁸.

L'usage d'un pseudonyme n'est pas apparu avec les réseaux sociaux ; il existe depuis longtemps et pour diverses raisons. Voici quelques illustrations. Premièrement, le pseudonyme artistique est une pratique légitime pour des noms difficiles à retenir ou à prononcer, par exemple « Apollinaire » a été jugé préférable à « Wilhelm Albert Popowski de la Selva de Appolinaris de Waz-Kostrowitzky »¹⁹. Deuxièmement, il peut être valorisant, comme pour certaines femmes à certaines époques qui avaient recours à un pseudonyme masculin, « George Sand » pour « Aurore Dupin »²⁰ par exemple. Troisièmement, le pseudonyme peut être utilisé par prudence, discrétion, voire pour atteindre un certain anonymat. Dans le domaine du journalisme, il s'agissait d'une protection essentielle contre l'absolutisme qui permettait de s'exprimer librement²¹. En quatrième lieu, le pseudonyme peut être utilisé comme avatar ou alias pour incarner une identité ludique sur internet ou dans les jeux et ainsi permettre de se sentir à l'aise dans une société de surveillance et d'auto-surveillance de plus en plus intrusive²².

Ce quatrième exemple est relatif à l'usage du pseudonymat sur internet. À ce sujet, le Groupe de l'article 29 (ci-après « Groupe 29 » ; « G29 ») a émis des avis et recommandations à destination des législateurs, des fournisseurs de services et des utilisateurs. Il s'agit d'un acteur créé au niveau de l'Union européenne par la Directive 95/46/CE²³ pour traiter des questions relatives à la protection de la vie privée et des données personnelles, jusqu'à l'entrée en vigueur du RGPD²⁴ le 25 mai 2018. Le G29 invite les États à introduire le droit à l'anonymat, à savoir le « droit d'agir sur un service de réseautage social sous un pseudonyme sans avoir à révéler sa véritable identité aux autres utilisateurs, ou au public le plus large »²⁵. Par ailleurs, il conseille

¹⁷Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la Directive 95/46/CE, *J.O.U.E.*, 27 avril 2016, art. 4.

¹⁸M. UNTERSINGER, *op. cit.*, p. VII (préface de B. BAYART).

¹⁹B. MOUFFE, *Le droit au mensonge*, Bruxelles, Larcier, 2017, p. 311.

²⁰B. MOUFFE, *op. cit.*, pp. 312-313.

²¹B. MOUFFE, *op. cit.*, p. 313.

²²B. MOUFFE, *op. cit.*, p. 316.

²³Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *J.O.C.E.*, 23 novembre 1995.

²⁴Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité.

²⁵Avis 5/2009 du Groupe de l'Article 29 sur les réseaux sociaux en ligne, 12 juin 2009, disponible sur https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf.

aux utilisateurs de ne pas hésiter à employer un pseudonyme et de varier celui-ci selon les plateformes.

L'usage de pseudonyme sur les réseaux sociaux est donc approuvé et même encouragé, notamment par le G29. Toutefois, cet usage n'est pas sans conséquences. En effet, le fait que la véritable identité de l'auteur ne soit pas connue peut entraîner certaines difficultés procédurales.

Section 2 : Réseaux sociaux

De manière générale, les réseaux sociaux sont considérés comme faisant partie de la catégorie des « services », et plus spécifiquement des « services proposés sur internet »²⁶. On peut classer ces services en deux catégories : d'une part les services de référencement de contenus, tels que les moteurs de recherche et les agrégateurs d'informations, et d'autre part les services de diffusion de contenus, incluant les forums de discussion, les sites collaboratifs, les réseaux sociaux et les plateformes de partage²⁷.

Le G29 a défini les réseaux sociaux comme des « plateformes de communication en ligne qui permettent à tout internaute de rejoindre ou de créer des réseaux d'utilisateurs ayant des opinions similaires et/ou intérêts communs »²⁸. Ces réseaux sociaux offrent la possibilité de publier son propre contenu, tel que des photos, des chroniques, des commentaires, de la musique, des vidéos ou des liens vers d'autres sites²⁹. Ils fonctionnent grâce à l'utilisation d'outils fournissant une liste de contacts pour chaque utilisateur avec une possibilité d'interagir entre eux³⁰. La caractéristique essentielle d'un réseau social réside donc dans sa capacité à permettre aux utilisateurs d'entrer en contact avec d'autres utilisateurs, que ce soit avec une catégorie spécifique (comme les amis Facebook), avec l'ensemble des utilisateurs, voire avec

²⁶T. LEONARD, « Les réseaux sociaux face à l'exonération de responsabilité des intermédiaires de l'internet : une application délicate », in *Les réseaux sociaux et le droit*, Bruxelles, Larcier, 2014, pp. 215-218.

²⁷*Ibid.*

²⁸Avis 5/2009 du Groupe de l'Article 29 sur les réseaux sociaux en ligne, 12 juin 2009, disponible sur https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf.

²⁹C. CASTETS-RENARD, « Titre 2 - Régulation des contenus des plateformes », in *Droit du marché unique numérique et intelligence artificielle*, 1^{re} édition, Bruxelles, Bruylant, 2020, p. 163.

³⁰Avis 5/2009 du Groupe de l'Article 29 sur les réseaux sociaux en ligne, 12 juin 2009, disponible sur https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf.

quiconque ayant accès au contenu. Cela crée ainsi une zone de partage virtuelle où les individus peuvent interagir les uns avec les autres³¹.

Les plateformes de réseaux sociaux ont, par ailleurs, fondamentalement changé la structure d'internet avec le temps. Auparavant, le web 1.0 se caractérisait par des pages relativement statiques, conçues et modifiées par des professionnels de l'informatique³², tandis que le web 2.0, apparu dans les années 2006-2007, est davantage axé sur les interactions entre utilisateurs³³. En effet, depuis leur émergence, les réseaux sociaux ont accordé une place prépondérante aux internautes, qui jouent un rôle actif, contributif et dynamique dans la production et la publication de contenus³⁴. Les réseaux sociaux permettent dès lors de « mettre en relation différents types d'utilisateurs, d'offrir des services en ligne adaptés aux préférences des utilisateurs et fondés sur des données fournies par les utilisateurs, de classer ou de référencer des contenus, notamment au moyen d'algorithmes, des biens et des services proposés ou mis en ligne par des tiers, de réunir plusieurs parties en vue de la vente d'un bien, de la prestation d'un service ou encore de l'échange ou du partage de contenus, d'informations, de biens ou de services »³⁵.

Les avantages de l'apparition des réseaux sociaux sont soulignés par la Commission européenne dans une Communication de 2016 sur les plateformes en ligne et le marché unique numérique³⁶. On retrouve, par exemple, « les gains d'efficacité, l'élargissement du choix offert aux consommateurs, la compétitivité entre entreprises, la possibilité pour les citoyens de participer à la vie sociale et démocratique en facilitant l'accès à l'information »³⁷.

³¹T. LEONARD, *op. cit.*, p. 124.

³²E. MONTERO, « La responsabilité des prestataires intermédiaires sur les réseaux », *R.D.T.I.*, 2008/32., p. 365.

³³F. GEORGE et J. HUBIN, « Les prestataires intermédiaires de la société de l'information face au droit commun de la responsabilité extracontractuelle », *A&M*, 2017/3, p. 224.

³⁴F. GEORGE et J. HUBIN., *op. cit.*, p. 217.

³⁵Résolution du Parlement européen du 15 juin 2017 sur les plateformes en ligne et le marché unique numérique (2016/2276(INI)).

³⁶Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions, « Les plateformes en ligne et le marché unique numérique – Perspectives et défis pour l'Europe », *COM* (2016) 288 final.

³⁷C. CASTETS-RENARD, *op. cit.*, pp. 169-170.

Chapitre 2 : Libertés fondamentales en tension sur les réseaux sociaux

Les réseaux sociaux, caractéristiques du web 2.0, offrent une zone de partage virtuelle aux utilisateurs afin de leur permettre d'interagir entre eux. Certes, le pseudonymat leur offre une liberté d'expression et permet la protection de certains utilisateurs, mais il peut aussi faciliter la diffusion de propos injurieux ou l'adoption de comportements illicites sur internet. Le défi est alors de trouver un équilibre entre la liberté d'expression des utilisateurs agissant sous anonymat et l'atteinte à la vie privée d'autres utilisateurs.

Dans ce chapitre, nous analyserons deux libertés fondamentales dans le contexte des réseaux sociaux, à savoir, le droit à la liberté d'expression et le droit à la vie privée. Dans un premier temps, nous aborderons le droit à la liberté d'expression. Nous en définirons le champ d'application matériel, les restrictions possibles, ainsi que son application aux réseaux sociaux. Ensuite, nous effectuerons le même schéma d'analyse pour le droit à la vie privée. Enfin, nous tenterons d'analyser l'équilibre entre ces deux libertés fondamentales.

Section 1 : Droit à la liberté d'expression

La puissance de l'expression réside dans sa capacité à jouer un rôle essentiel dans le développement des compétences individuelles nécessaires à l'épanouissement de l'homme, ainsi que dans sa légitimation de la parole dans la délibération démocratique³⁸. Une solide protection de la liberté d'expression est donc essentielle.

Le droit à la liberté d'expression est consacré par l'article 19 de la Constitution belge qui garantit la liberté de manifester ses opinions³⁹. L'article 10 de la Convention européenne des droits de l'homme (ci-après « CEDH ») consacre également ce droit. Cet article établit que toute personne a droit à la liberté d'expression, englobant la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées, sans ingérence d'autorités publiques et sans considération de frontières⁴⁰. Selon la Cour européenne des droits de

³⁸K. GELBER et S. J. BRINSON, « Digital dualism and the 'speech as thought' paradox », in *Free speech in the digital age* (sous la dir. de S.J. BRISON et K. GELBER), Oxford University Press, p. 26.

³⁹Const., art. 19.

⁴⁰Convention de sauvegarde des Droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950, approuvée par la loi du 13 mai 1955, *M.B.*, 19 août 1955, art.10, §1.

l'homme, cette liberté est une condition fondamentale pour le progrès des sociétés démocratiques et pour le développement de chaque individu⁴¹.

Sous-section 1 : Champ d'application matériel

Le champ d'application matériel de l'article 10 de la CEDH comprend, d'une part, la liberté d'opinion. Dans l'arrêt *Handyside c. Royaume-Uni*, la Cour a indiqué qu'il s'agissait de la volonté affichée de tolérance et d'ouverture quant au contenu des opinions exprimées : « Opinions accueillies avec faveur ou considérées comme inoffensives mais aussi celles qui heurtent, choquent, inquiètent. »⁴² D'autre part, il inclut aussi la liberté de recevoir ou de communiquer des informations ou des idées.

Sous-section 2 : Restrictions

Le droit à la liberté d'expression est certes un droit fondamental, mais il n'est pas absolu⁴³. La Convention européenne des droits de l'homme autorise et prévoit des restrictions à celui-ci. Le deuxième paragraphe de l'article 10 accorde en effet aux États membres la possibilité de restreindre le droit à la liberté d'expression⁴⁴.

Toutefois, les potentielles exceptions doivent respecter trois conditions. Tout d'abord, il y a le principe de légalité qui entend que l'ingérence doit être prévue par la loi. La loi doit être entendue au sens matériel. Il doit s'agir d'une norme prévisible, suffisamment claire, précise et accessible. Ensuite, le principe de légitimité doit être pris en compte. L'ingérence dans le droit à la liberté d'expression doit poursuivre un but légitime expressément prévu par l'article 10, tel que « la sécurité nationale, l'intégrité territoriale, la protection de la santé ou de la morale, la protection de la réputation ou des droits d'autrui, empêcher la divulgation d'informations confidentielles ou la garantie de l'autorité et de l'impartialité du pouvoir judiciaire »⁴⁵. Enfin, le principe de nécessité doit être respecté, selon lequel l'ingérence doit être nécessaire dans une société démocratique. La Cour a mis en place, à travers sa jurisprudence, trois critères à prendre

⁴¹Cour eur. D.H., arrêt *Handyside c. Royaume-Uni*, 7 décembre 1976, n° 5493/72, §49.

⁴²Cour eur. D.H., arrêt *Handyside c. Royaume-Uni*, 7 décembre 1976, n° 5493/72, §49.

⁴³Q. VAN ENIS, « Chapitre 4. - Filtrage et blocage de contenus sur Internet au regard du droit à la liberté d'expression », in *L'Europe des droits de l'homme à l'heure d'Internet* (sous la dir. C. DE TERWANGNE et Q. VAN ENIS), 1^{re} édition, Bruxelles, Bruylant, 2019, p. 146.

⁴⁴F. ERNOTTE, *Le droit des réseaux sociaux*, Bruxelles, Larcier, 2021, p. 50.

⁴⁵Convention de sauvegarde des Droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950, approuvée par la loi du 13 mai 1955, *M.B.*, 19 août 1955, art. 10, §2.

en considération lors de l'analyse de cette dernière condition. Premièrement, il doit y avoir l'existence d'un besoin social impérieux⁴⁶. Deuxièmement, l'ingérence doit être proportionnée⁴⁷. Troisièmement, il doit s'agir de la mesure la moins attentatoire à la liberté d'expression⁴⁸.

Il s'agit donc de restrictions qui sont évaluées au cas par cas.

Sous-section 3 : Application du droit à la liberté d'expression aux réseaux sociaux

Au 21^e siècle, l'expression publique n'a jamais été aussi accessible⁴⁹. Peu coûteux, les réseaux sociaux offrent en effet un espace d'échange et de communication relativement illimité⁵⁰. Cette évolution peut avoir des conséquences positives pour l'exercice du droit à la liberté d'expression, mais elle suscite également des risques d'abus⁵¹. Internet « permet le meilleur pour les droits et libertés tout en laissant craindre le pire »⁵².

Premièrement, il est important de se rappeler qu'internet a fait émerger de nouveaux moyens de communication. La Cour européenne des droits de l'homme l'a d'ailleurs souligné dans l'arrêt *Musico c. Italie* en affirmant que « la diffusion d'internet et des systèmes d'échange de courriers électroniques a fait naître des possibilités de communication qui n'existaient pas auparavant »⁵³. Par ailleurs, dans un autre arrêt, *K.U. c. Finlande*, la Cour reconnaît que le développement rapide des technologies de la communication a facilité la commission de crimes ou délits classiques et conduit à l'émergence de nouveaux types d'infractions⁵⁴. Certains utilisateurs abusent parfois de leur droit à la liberté d'expression, en utilisant ces nouveaux moyens de communication pour nuire à autrui⁵⁵. Le cyberharcèlement, les propos racistes et les discours de haine en sont des exemples.

⁴⁶Cour eur. D.H., arrêt *Glor c. Suisse*, 30 avril 2009, n° 13444/04, §94.

⁴⁷Cour eur. D.H., arrêt *Glor c. Suisse*, 30 avril 2009, n° 13444/04, §94.

⁴⁸Cour eur. D.H., arrêt *Glor c. Suisse*, 30 avril 2009, n° 13444/04, §94.

⁴⁹F. ERNOTTE, *op. cit.*, p. 13.

⁵⁰K. GELBER et S.-J. BRINSON, *op. cit.*, p. 26.

⁵¹Z. KARAMBIRI, « La responsabilité liée aux contenus postés dans les blogs », *R.D.T.I.* 2009/3, n° 36 - 20 octobre 2009, p. 29.

⁵²M. LARCHE, « Le Digital Services Act : un pas européen supplémentaire dans la lutte contre l'incitation à la haine et la violence sur les réseaux sociaux », *Rev. Aff. Eur.*, 2021/1, p. 140-141.

⁵³Cour eur. dr. h., arrêt *Muscio c. Italie*, 13 novembre 2007, n° 31358/03.

⁵⁴Cour eur. dr. h., arrêt *K.U. c. Finlande*, 2 décembre 2008, n° 2872/02, § 22.

⁵⁵F. ERNOTTE, *op. cit.*, p. 41.

Face à ces comportements, le débat surgit en doctrine sur la question de limiter ou non le droit à la liberté d'expression sur les réseaux sociaux.

L'auteur J. ENGLEBERT s'oppose à l'idée de restreindre le droit à la liberté d'expression sur les réseaux sociaux. Il conteste la mise en place de limitations, car selon lui les discours de haine ne sont pas devenus plus agressifs ou attentatoires avec le développement d'internet⁵⁶. Il estime que la propagation de cette haine résulte avant tout de facteurs culturels et économiques de la société⁵⁷. Selon lui, instaurer des limitations à la liberté d'expression pourrait laisser une place à l'arbitraire⁵⁸. S'il devait toutefois y avoir une limite à la liberté d'expression, l'auteur préconise de la baser sur la contribution de l'expression litigieuse à un débat d'intérêt général, notamment dans les domaines politiques et la gestion de la cité, la santé, l'environnement, l'administration, etc.⁵⁹. Toute mesure d'ingérence doit, selon lui, être élaborée avec prudence et mesure⁶⁰, étant donné que le droit à la liberté d'expression joue un rôle essentiel dans les sociétés démocratiques.

D'autres auteurs reconnaissent l'importance de la liberté d'expression dans une société démocratique, tout en considérant que des limites doivent être apportées, dans certaines circonstances, pour éviter les dérives. L'inaction face à de tels comportements pourrait entraîner l'exclusion de certaines personnes dans l'espace public d'internet, menaçant ainsi le débat démocratique et favorisant la loi du plus fort, ce qui, pour ces auteurs, serait inacceptable⁶¹. C'est également le constat de D. K. CITRON qui indique que les individus victimes de cyberharcèlement se retirent des réseaux sociaux, ferment leurs blogs ou autres sites⁶². Une étude réalisée par Amnesty International révèle que 76% des femmes victimes de violences en ligne ont dû modifier leur manière d'utiliser internet, voire pour 32% d'entre elles cesser d'y exprimer leur opinion⁶³.

⁵⁶J. ENGLEBERT, « Titre 4 – La liberté d'expression à l'heure de l'Internet », in *Vie privée, liberté d'expression et démocratie dans la société numérique*, Bruxelles, Editions Larcier, 2020, p. 138.

⁵⁷J. ENGLEBERT, *op. cit.*, p. 139.

⁵⁸J. ENGLEBERT, *op. cit.*, p. 141.

⁵⁹J. ENGLEBERT, *op. cit.*, p. 145.

⁶⁰J. ENGLEBERT, *op. cit.*, p. 149.

⁶¹M. LEROY et F. HAINAUT, documentaire « #SalePute », Belgique : RTBF, Proximus, Arte., 2021, visionné le 3 août 2022, min 46.

⁶²D. K. CITRON, « Restricting speech to protect it », in *Free speech in the digital age* (sous la dir. de S.J. BRISON et K. GELBER), Oxford University Press, 2019, pp. 123.

⁶³Amnesty International France, « Harcèlement en ligne : l'impact inquiétant », disponible sur <https://www.amnesty.fr/discriminations/actualites/des-femmes-du-monde-entier-font-etat-de-stress-dangoisse>, consulté le 29 juillet 2023.

Ce débat porte sur les potentielles restrictions du droit à la liberté d'expression sur internet en général. Mais qu'en est-il de l'usage de la liberté d'expression lorsqu'il est mis en œuvre par un auteur anonyme ? La Cour européenne des droits de l'homme a abordé la question dans son arrêt Delfi⁶⁴ précité. Cet arrêt opposait d'une part la société Delfi, propriétaire d'un grand portail d'actualités en ligne en Estonie, et d'autre part l'actionnaire d'une société qui avait fait l'objet de nombreuses critiques après la publication d'un article sur ce portail d'actualités le 24 janvier 2006. L'actionnaire avait demandé que Delfi retire les commentaires et lui verse une indemnité. La société a retiré les commentaires mais refusait de payer l'indemnité. Face à ce refus, l'actionnaire a intenté une action contre Delfi. La juridiction a donné raison au plaignant, estimant que la société aurait dû retirer ses commentaires injurieux de sa propre initiative et la condamnant dès lors au paiement d'une indemnité de 320 euros⁶⁵.

En réaction, Delfi décida de saisir la Cour européenne des droits de l'homme pour cause de violation de l'article 10 de la Convention relatif au droit à la liberté d'expression⁶⁶. La Cour, dans son arrêt du 10 octobre 2013, conclut à la non-violation de cet article. La société demanda alors le renvoi de l'affaire devant la Grande Chambre. Le 16 juin 2015, la Grande Chambre de la Cour rendit son arrêt dans lequel elle indiqua, dans un premier temps, que « les avantages d'internet s'accompagnent d'un certain nombre de risques : propos clairement illicites (diffamatoires, haineux, appelant à la violence, etc.) »⁶⁷. Dans la suite de son raisonnement, la Cour estimait que, puisque Delfi autorisait des commentaires anonymes et qu'elle trouvait un intérêt commercial à l'existence de ces espaces contributifs, il était « raisonnable » que l'entreprise soit déclarée responsable en lieu et place des auteurs des propos litigieux⁶⁸.

L'enseignement de cet arrêt est important. Tout d'abord, il souligne l'importance fondamentale du droit à la liberté d'expression sur internet permettant aux individus de s'exprimer librement, y compris lorsqu'ils sont anonymes. En revanche, l'arrêt insiste sur la nécessité d'accorder des recours effectifs aux personnes lésées par des propos diffamatoires⁶⁹.

⁶⁴Cour eur. D.H., arrêt Delfi AS c. Estonie, 10 octobre 2013, n° 64569/09.

⁶⁵Cour eur. D.H., arrêt Delfi AS c. Estonie, 10 octobre 2013, n° 64569/09, §27.

⁶⁶Cour eur. D.H., arrêt Delfi AS c. Estonie, 10 octobre 2013, n° 64569/09, §59.

⁶⁷Cour eur. D.H., arrêt Delfi AS c. Estonie, 16 juin 2015, n° 64569/09.

⁶⁸F. TREGUER, « Chapitre 8. - Anonymat et chiffrement, composantes essentielles de la liberté de communication », in *L'Europe des droits de l'homme à l'heure d'Internet* (sous la dir. de C. TERWANGNE et Q. VAN ENIS), 1^{re} édition, Bruxelles, Bruylant, 2019, p. 313.

⁶⁹Cour eur. D.H., arrêt Delfi AS c. Estonie du 10 octobre 2013, n° 64569/09, §111.

En somme, le débat sur la liberté d'expression sur les réseaux sociaux et l'anonymat des auteurs reste complexe et suscite des opinions divergentes.

Section 2 : Droit à la vie privée

Le droit à la vie privée est consacré au niveau national par l'article 22 de la Constitution⁷⁰, garantissant le droit au respect de sa vie privée et familiale, sous réserve des cas et conditions fixés par la loi. Au niveau européen, l'article 8 de la Convention européenne des droits de l'homme reconnaît également ce droit, protégeant le respect de la vie privée, familiale, du domicile et de la correspondance de chacun⁷¹.

La notion de vie privée est large et complexe. D'après M. UNTERSINGER, le droit à la vie privée englobe un ensemble de prérogatives essentielles au développement de la personnalité de l'individu et à son autonomie au sein d'une société en constante évolution, dans le but de garantir la viabilité de nos démocraties⁷².

La jurisprudence de la Cour européenne des droits de l'homme interprète ce terme comme permettant d'englober le droit à l'intimité, le droit de poursuivre librement le développement et l'accomplissement de sa personnalité⁷³, le droit de nouer et développer des relations avec d'autres humains et le droit de resserrer les liens avec le monde extérieur⁷⁴.

Par ailleurs, des juristes américains, S. WARREN et L. BRANDEIS, ont tenté de définir sa portée. Il s'agirait de la première définition moderne de la vie privée⁷⁵. Selon eux, la vie privée englobe trois concepts : le secret, la quiétude et l'autonomie⁷⁶. Le « secret » se réfère à la « capacité à contrôler la collecte et l'utilisation de ses données personnelles ainsi que la possibilité de décider quand partager ou cacher ses attitudes, croyances, comportements et opinions »⁷⁷. La « quiétude » permet aux individus de « préserver une sphère personnelle en s'isolant de la

⁷⁰ Const. art. 22

⁷¹ Convention de sauvegarde des Droits de l'homme et des libertés fondamentales précitée, art. 8.

⁷² Y. POULLET, « En guise de préface », in *Le droit à la vie privée* (sous la dir. de B. DOCQUIR), Bruxelles, De Boeck-Larcier, 2008, p.10.

⁷³ Cour eur. D.H., arrêt Smimova c. Russie, 24 avril 2003, n° 46133/99 et 48183/99, §95 ; Cour eur. D.H., arrêt Sidabras et Dziautas c. Lituanie, 27 juillet 2004, n° 55480/00 et 59330/00, §43.

⁷⁴ Cour eur. D.H., arrêt Niemietz c. Allemagne 16 décembre 1992, n°13710/88, §29.

⁷⁵ M. UNTERSINGER, *op. cit.*, p. 4.

⁷⁶ *Ibid.*

⁷⁷ Brim & Ruebhausen, 1965, cités dans Rochelandet, 2010.

société et en contrôlant l'accessibilité à soi »⁷⁸. Enfin, l'« autonomie » se réfère à l'« identité, les opinions et la manière de vivre des individus »⁷⁹.

La Cour européenne des droits de l'homme, dans son arrêt *Pretty c. Royaume-Uni*, a souligné l'importance du droit à la vie privée, en affirmant que ce droit est la condition préalable à toutes les autres libertés. En effet, il établit les conditions de l'épanouissement des libertés individuelles et du respect de la dignité humaine, qui est une valeur fondamentale pour la démocratie⁸⁰.

Sous-section 1 : Champ d'application matériel

Concernant le champ d'application matériel, le droit à la vie privée couvre aussi bien la confidentialité et l'intimité des individus et des familles, que le développement personnel à travers les interactions sociales, y compris sur le plan professionnel, allant même jusqu'à un droit à l'épanouissement personnel⁸¹.

Le droit à la vie privée comporte deux aspects essentiels. D'une part, il impose des obligations négatives à charge des autorités publiques des États membres en les empêchant de porter atteinte de manière arbitraire à l'exercice du droit à la vie privée des individus⁸². D'autre part, il prévoit des obligations positives dans le chef des États membres en exigeant qu'ils garantissent le respect au droit à la vie privée par autrui⁸³.

Sous-section 2 : Restrictions

Tout comme le droit à la liberté d'expression évoqué précédemment, le droit à la vie privée est un droit fondamental mais il n'est pas absolu. Dans son second paragraphe, l'article 8 de la CEDH prévoit la possibilité de restreindre ce droit, moyennant le respect d'un ensemble de conditions⁸⁴. L'ingérence éventuelle dans le droit à la vie privée doit être d'une part prévue par

⁷⁸*Ibid.*

⁷⁹*Ibid.*

⁸⁰Cour eur. D.H., arrêt *Pretty c. Royaume-Uni*, 29 avril 2002, n° 2346/02, §61.

⁸¹E. CORNU et B. DOCQUIR, « IV. - Le respect de la vie privée », in *Les réseaux sociaux et le droit* (sous la dir. de M. SALMON), 1^{re} édition, Bruxelles, Larcier, 2014, p. 107.

⁸²A. ARAMAZANI, « Le droit à l'oubli et internet », *R.D.T.I.*, 2011/2, n° 43, p. 40 ; Cour eur. D.H., arrêt *Marckx c. Belgique*, 13 juin 1979, n° 6833/74.

⁸³*Ibid.*

⁸⁴A. FARCY, « Vie privée et liberté d'expression : application aux publications et « likes » sur Facebook d'un travailleur », *R.D.T.I.*, 2018/2, p. 122.

la loi, et d'autre part constituer une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre, à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui⁸⁵.

Sous-section 3 : Application du droit à la vie privée aux réseaux sociaux

On retrouve plusieurs applications du droit à la vie privée sur les réseaux sociaux. En voici quelques-unes.

Tout d'abord, certains utilisateurs cherchent à protéger leur vie privée en voulant éviter que leurs données personnelles soient utilisées par les plateformes, dans un but commercial par exemple. Cette application du droit à la vie privée est souvent liée à la question de l'anonymat, car certains individus ne souhaitent pas divulguer leurs données personnelles⁸⁶. On constate depuis quelques années une augmentation des réglementations à ce sujet, notamment le Règlement général sur la protection des données⁸⁷, qui entend encadrer l'utilisation des données personnelles⁸⁸. Ce règlement européen a été transposé en droit belge par la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel⁸⁹. Cet instrument impose des obligations à charge du responsable du traitement et du sous-traitant des données.

On peut également mentionner le droit à l'oubli numérique. Ce droit, consacré par l'article 17 RGPD⁹⁰, rassemble l'ensemble des instruments, tant juridiques que technologiques, permettant à un individu d'obtenir ou ré-obtenir la maîtrise de ses données personnelles dispersées sur internet⁹¹. Avec la quantité croissante d'informations et de données circulant quotidiennement sur internet, la question est de savoir comment gérer et maîtriser ce flux d'informations personnelles⁹².

⁸⁵Convention de sauvegarde des droits de l'homme et des libertés fondamentales précitée, art. 8, §2.

⁸⁶M. UNTERSINGER, *op. cit.*, p. 3.

⁸⁷Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité.

⁸⁸F. ERNOTTE, *op. cit.*, p. 82.

⁸⁹Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *M.B.*, 5 septembre 2018.

⁹⁰Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, art. 17.

⁹¹F. ERNOTTE, *op. cit.*, p. 102.

⁹²A. ARAMAZANI, *op. cit.*, p. 35.

Enfin, il arrive que les utilisateurs des réseaux sociaux soient confrontés à des situations où leur droit à la vie privée est entravé par les actions d'autres utilisateurs sur la plateforme. Un exemple concret en est le cyberharcèlement, où un ou plusieurs utilisateur(s) ne respecte(nt) pas la tranquillité et l'épanouissement d'un autre utilisateur sur la plateforme.

Comme on le voit, « anonymat et vie privée sont très souvent associés, et pour cause. Le premier est un moyen de préserver la seconde »⁹³.

Section 3 : Équilibre entre le droit à la liberté d'expression et le droit à la vie privée sur les réseaux sociaux

Les droits à la liberté d'expression et à la vie privée sont deux droits fondamentaux protégés tant par la Constitution belge que par la Convention européenne des droits de l'homme. Lorsque ces droits sont exercés sans porter atteinte à autrui, il n'y a pas de raison de restreindre leur portée. Cependant, sur les réseaux sociaux, des atteintes peuvent être causées à des individus lorsque quelqu'un utilise sa liberté d'expression pour insulter ou harceler quelqu'un d'autre, entraînant ainsi la violation du droit à la vie privée de la personne visée.

Cette situation met en évidence la tension existant entre ces deux libertés fondamentales sur les réseaux sociaux. Trouver des solutions pour prévenir et réprimer les abus, tout en respectant les droits des individus de se prononcer et de débattre, constitue un défi majeur dans l'environnement numérique⁹⁴.

À ce sujet, le Comité des ministres du Conseil de l'Europe, prenant en compte la complexité de l'utilisation de pseudonymes sur les réseaux sociaux, reconnaît que l'utilisation de pseudonymes peut présenter à la fois des avantages et des risques en matière de droits fondamentaux⁹⁵. Ainsi, le droit d'utiliser des pseudonymes est considéré comme crucial pour préserver la liberté d'expression, le droit de communiquer et de recevoir des informations, ainsi

⁹³M. UNTERSINGER, *op. cit.*, p. 55.

⁹⁴J. WEINSTEIN, « Cyber harassment and free speech: drawing the line online », in *Free speech in the digital age* (sous la dir. de S.J. BRISON et K. GELBER), Oxford University Press, 2019, p. 69.

⁹⁵ Recommandation comité min. n°Rec (2012)4, du Comité des Ministres aux États membres sur la protection des droits de l'homme dans le cadre des services de réseaux sociaux, 4 avril 2012, disponible sur https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805caaad.

que le droit au respect de la vie privée⁹⁶. Le Comité estime également que, dans certains cas, il peut être nécessaire pour les autorités d'avoir accès à la véritable identité d'un internaute. Toutefois, cela doit se faire en conformité avec les garanties juridiques appropriées pour le respect des droits et libertés fondamentales de l'individu⁹⁷.

La Cour de justice de l'Union européenne (ci-après « C.J.U.E. ») a eu l'occasion de se prononcer au sujet de cet équilibre si difficile à atteindre en pratique. Dans son arrêt *Tobias Mc Fadden c. Sony Music Entertainment Germany GmbH* du 15 septembre 2016, la C.J.U.E. estime que le droit européen ne « s'oppose pas à l'adoption d'une injonction judiciaire consistant à exiger d'un fournisseur d'accès à un réseau accessible au public de sécuriser la connexion à internet au moyen d'un mot de passe afin que les utilisateurs de ce réseau soient obligés de révéler leur identité et ne puissent donc pas agir anonymement »⁹⁸. La Cour indique que l'article 8 de la Convention européenne des droits de l'homme implique une obligation positive à charge des États d'adopter des dispositions en matière pénale qui sanctionnent effectivement les infractions contre les personnes. Il appartient donc à l'État de prendre en considération les dérives potentielles afin d'assurer le respect des droits et libertés⁹⁹.

Dans l'arrêt *K.U. c. Finlande*, la Cour européenne des droits de l'homme a ainsi estimé qu'une protection pratique et effective du requérant impliquait l'adoption de mesures efficaces pour identifier l'auteur¹⁰⁰. Dans cette affaire, une annonce anonyme à caractère sexuel avait été publiée au sujet d'un mineur sur un site de rencontre sur internet. Le père du mineur a fait une demande à la police pour pouvoir identifier l'auteur de ladite annonce. Le fournisseur d'accès refusa de donner l'identité. À l'époque des faits, la législation finlandaise ne permettait pas aux autorités d'obliger les fournisseurs d'accès à identifier l'auteur anonyme¹⁰¹. La Finlande a été condamnée pour avoir violé l'article 8 de la Convention, car l'État n'avait pas respecté son

⁹⁶ Recommandation comité min. n°Rec (2012)4, du Comité des Ministres aux États membres sur la protection des droits de l'homme dans le cadre des services de réseaux sociaux, 4 avril 2012, disponible sur https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805caaad.

⁹⁷ Recommandation comité min. n°Rec (2012)4, du Comité des Ministres aux États membres sur la protection des droits de l'homme dans le cadre des services de réseaux sociaux, 4 avril 2012, disponible sur https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805caaad

⁹⁸ C.J.U.E., arrêt *Tobias Mc Fadden / Sony Music Entertainment Germany GmbH*, 15 septembre 2016, C-484/14, § 102.

⁹⁹ S. TURGIS, « La coexistence d'internet et des médias traditionnels sous l'angle de la Convention européenne des droits de l'homme », *Rev. Trim. D.H.*, 2013/93, p. 18.

¹⁰⁰ Cour eur. D.H., arrêt *K.U. c. Finlande*, 2 décembre 2008, n°2872/02, § 49.

¹⁰¹ F. DUMORTIER et C. FORGET, « Criminalité informatique », *R.D.T.I.*, 2017/3-4, n° 68 - 12 novembre 2018, p. 215.

obligation positive¹⁰². La Cour semble ainsi privilégier le respect des droits d'autrui sur le droit à l'anonymat.

Une tendance jurisprudentielle semble donc se dessiner. Il n'y a aucun inconvénient à ce qu'un individu exerce son droit à la liberté d'expression, peu importe que ce dernier soit couvert d'anonymat ou non. Toutefois, en cas d'atteinte au droit à la vie privée d'un autre utilisateur, l'individu en cause ne devrait pas bénéficier d'une impunité totale au nom de la liberté d'expression. Son identité devrait pouvoir être révélée afin de le sanctionner.

En conclusion, les droits à la liberté d'expression et à la vie privée sont indispensables dans une société démocratique et jouent un rôle essentiel dans l'environnement numérique actuel. Néanmoins, leur coexistence peut parfois se révéler fragile en raison des abus pouvant résulter de leur utilisation.

¹⁰²Cour eur. D.H., arrêt K.U. c. Finlande, 2 décembre 2008, n° 2872/02, § 46.

Partie 2 : Procédures d'identification des auteurs d'infractions sur les réseaux sociaux

Cachés derrière l'anonymat, les individus peuvent avoir le sentiment d'agir en totale impunité¹⁰³, ce qui pourrait les pousser à commettre toutes sortes de « débordements »¹⁰⁴. Toutefois, comme décrit dans la première partie de ce mémoire, la tendance se dessine, selon laquelle un individu anonyme ne devrait pas porter atteinte aux droits d'autrui et rester dans l'impunité. Ces atteintes, considérées comme des actes illégaux dans le monde physique, doivent aussi l'être dans le monde virtuel¹⁰⁵. Des techniques devraient exister pour permettre de révéler l'identité de l'individu en question afin de l'attirer en justice et qu'il réponde de ses actes.

Il existe cependant plusieurs obstacles qui entravent la recherche de l'identité d'un individu, et plus spécifiquement en matière de répression des infractions sur internet. En voici quelques-uns.

Tout d'abord, la loi pénale et la procédure pénale peuvent rencontrer des difficultés à suivre les nombreuses et rapides évolutions technologiques de notre société¹⁰⁶. Les autorités judiciaires sont souvent limitées par un cadre juridique qui a été conçu à une autre époque, pour des crimes commis dans le monde physique¹⁰⁷. Il y a en effet un décalage entre le droit et la réalité technique du web, dû à l'écart temporel entre le temps instantané d'internet, en constante évolution, et le temps lent du droit, qui s'évalue en années¹⁰⁸.

¹⁰³ F. TREGUER, *op. cit.*, p. 313.

¹⁰⁴ E. DERIEUX et A. GRANCHET, *Réseaux sociaux en ligne : aspects juridiques et déontologiques*, Wolters Kluwer, 2013, p. 189.

¹⁰⁵ Communiqué de presse de la Commission européenne : « Une Europe adaptée à l'ère du numérique : la Commission propose de nouvelles règles pour les plateformes numériques », 15 décembre 2020, disponible sur https://ec.europa.eu/commission/presscorner/detail/fr/ip_20_2347.

¹⁰⁶ 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*, Bruxelles, Bruylant, 2019, p. 133.

¹⁰⁷ V. FRANSEN et O. LEROUX, *op. cit.*, p. 133.

¹⁰⁸ E. BARBRY, « Le droit de l'Internet est devenu au fil des années un « droit spécial » », *Gaz. Pal.*, 23 octobre 2010, p.14.

Un autre obstacle à la répression sur les réseaux sociaux concerne la problématique de la territorialité. Internet n'a ni de frontières¹⁰⁹ ni d'ancrage territorial¹¹⁰, contrairement au droit qui demeure essentiellement national, et par conséquent lié à un territoire déterminé¹¹¹. Internet est certes considéré comme un espace autonome purement virtuel, il n'est toutefois pas totalement détaché des États. Comme nous le verrons, cet obstacle a suscité et continue de susciter des débats, ayant des conséquences dans le monde physique¹¹².

Par ailleurs, pour pouvoir réprimer les comportements illégaux, il faut savoir « qui est qui, et qui fait quoi »¹¹³. Cependant, les autorités ne peuvent contraindre une personne à donner l'accès à son profil d'utilisateur sur un réseau social car cela violerait son droit au silence. Le droit au silence, faisant partie du droit au procès équitable protégé par l'article 6 de la Convention européenne des droits de l'homme, implique le droit de ne pas témoigner contre soi-même, mais également le droit de ne pas contribuer à sa propre incrimination¹¹⁴.

Il convient également de rappeler que ces plateformes de réseaux sociaux sont des entreprises privées et non publiques. Cela signifie qu'elles ne doivent pas faire l'objet d'un contrat de gestion avec l'Etat¹¹⁵. Les nombreux défis liés au développement des réseaux sociaux dépendent, au départ, essentiellement du bon vouloir de ces plateformes¹¹⁶. Toutefois, comme l'indique O. BOGAERT, membre de la *Federal Computer Crime Unit* (ci-après « FCCU ») dans notre entretien, ces dernières sont à présent soumises à bon nombre d'obligations. Elles n'ont plus beaucoup de marge de manœuvre dans la décision de collaborer ou non¹¹⁷.

Enfin, les procédures d'identification d'un individu sur internet pourraient entraîner la communication de données personnelles par le prestataire de services aux autorités judiciaires. Les parties impliquées dans les procédures devront respecter les dispositions relatives à la

¹⁰⁹V. FRANSEN et O. LEROUX, *op. cit.*, p. 133.

¹¹⁰F. MARCHADIER, « Chapitre II - Le web », in *Les nouveaux pouvoirs*, 1^e édition, Bruxelles, Bruylant, 2017, p. 60.

¹¹¹E. DERIEUX et A. GRANCHET, *op. cit.*, p. 22.

¹¹²F. MARCHADIER, *op. cit.*, p. 66.

¹¹³M. UNTERSINGER, *op. cit.*, p. 12.

¹¹⁴Cass., 19 juin 2013, n° F-20130619-2 (P.12.1150.F).

¹¹⁵A. ADAM, « Anonymat et faux anonymat : comment identifier et poursuivre les auteurs de contenus haineux sur les réseaux sociaux », in *La régulation des contenus haineux sur les réseaux sociaux*, Anthemis, Limal, 2022, p. 87.

¹¹⁶*Ibid.*

¹¹⁷Voy. Annexe, question 5 de l'entretien avec Monsieur OLIVIER BOGAERT, membre à la *Federal Computer Crime Unit* (FCCU), le 31 juillet 2023.

protection des données personnelles, telles que le Règlement général sur la protection des données¹¹⁸, afin de maintenir un équilibre entre les intérêts en présence, à savoir le droit à la vie privée et le droit à la propriété¹¹⁹.

Eu égard à ces obstacles, comment trouver un équilibre entre la volonté des utilisateurs de ne pas révéler leur identité et la nécessité pour les autorités judiciaires de retrouver le responsable d'actes illégaux¹²⁰ ?

Cette seconde partie s'interroge sur les procédures permettant d'identifier l'auteur d'une infraction commise sur les réseaux sociaux.

Le premier chapitre portera sur le régime d'autorégulation des plateformes. Les chapitres suivants aborderont les procédures de corégulation entre les plateformes et les autorités judiciaires, permettant de révéler l'identité d'un individu. Le deuxième chapitre concernera l'obligation d'information applicable aux prestataires de services de la société de l'information prévue dans la Directive 2000/31/CE. Le troisième chapitre analysera, quant à lui, l'obligation de collaboration des plateformes prévue à l'article 46bis du Code d'instruction criminelle (ci-après « C.i.cr. »). Enfin, le dernier chapitre se focalisera sur les injonctions faites aux fournisseurs d'accès à internet en cas d'atteinte aux droits de propriété intellectuelle, prévues par les Directives 2001/29/CE et 2004/48/CE.

Chapitre 1 : Régime d'autorégulation des réseaux sociaux

L'autorégulation désigne « un mode d'encadrement d'une activité mis en place dans la détermination des règles et le contrôle de leur application, de leur propre initiative ou de manière volontaire, par ceux qui sont directement les principaux ou seuls concernés, exprimant ainsi leur sens de responsabilité tout en cherchant probablement, par la même occasion, à mieux

¹¹⁸Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité.

¹¹⁹B. DOCQUIR, « Titre 4 : Responsabilité et sécurité », in *Droit du numérique : contrats, innovation, données et sécurité*, Bruxelles, Larcier, 2018, p. 615.

¹²⁰Déclaration sur la liberté de la communication sur Internet adoptée par le Comité des Ministres lors de la 840e réunion des Délégués des Ministres, le 28 mai 2003.

garantir leur liberté »¹²¹. Les acteurs privés adoptent leurs propres règles¹²² afin de déterminer qui peut avoir accès à leur service et aux contenus¹²³.

Cette démarche d'élaboration de règles d'autorégulation est préconisée par le Comité des ministres du Conseil de l'Europe dans une Recommandation sur la protection des Droits de l'homme dans le cadre des services de réseaux sociaux. Les États membres y sont invités à « mettre en place des mécanismes d'autorégulation et de corégulation »¹²⁴.

Bien que ces procédures de régulation d'ordre privé soient encouragées, les prestataires ne sont pas totalement libres dans leur élaboration. Ces règles sont en effet souvent encadrées par des réglementations, voire des autorités indépendantes, mises en place au niveau européen¹²⁵.

Section 1 : Champ d'application

Les internautes, dès leur inscription sur le réseau social, consentent à ces normes¹²⁶. Ces règles, tantôt appelées « conditions générales d'utilisation », tantôt « standards de la communauté », ont pour vocation de réguler les comportements des individus sur les plateformes en indiquant quels comportements sont autorisés ou interdits. À travers ces règles, les prestataires informent les internautes, d'une part sur le caractère illicite de certains messages, et d'autre part sur la responsabilité pénale qui peut en découler¹²⁷. Cela a pour objectif général de garantir un espace sécurisé où l'on peut discuter librement.

Par exemple, les « standards de la communauté » de Facebook sont organisés en six catégories : violence et comportement criminel ; sécurité ; contenu répréhensible ; intégrité et authenticité ; respect de la propriété intellectuelle ; décisions et demandes relatives aux contenus. Ils sont ensuite divisés en sous-catégories indiquant quel contenu est considéré comme « non autorisé » et quel contenu « requiert des informations supplémentaires ou du contexte en vue de

¹²¹E. DERIEUX et A. GRANCHET, *op. cit.*, p. 73.

¹²²P. VAN OMMESELAGHE, « L'autorégulation : rapport de synthèse », in *L'autorégulation*, Bruxelles, Bruylant, 1995, pp. 233 et s.

¹²³F. MARCHADIER, *op. cit.*, p. 70.

¹²⁴Recommandation comité min. n°Rec (2012)4, du Comité des Ministres aux États membres sur la protection des droits de l'homme dans le cadre des services de réseaux sociaux, 4 avril 2012, disponible sur https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805caaad.

¹²⁵Y. POULLET, « Le temps du numérique, le temps du droit et le temps du droit du numérique », in *Guerre et paix* (sous la dir. de M. ANDRÉ), 1^{re} édition, Bruxelles, Larcier, 2023, pp. 475.

¹²⁶E. DERIEUX et A. GRANCHET, *op. cit.*, p. 88.

¹²⁷Y. POULLET, « La lutte contre le racisme et la xénophobie sur internet », *J.T.*, 2006/23, n° 6229, p. 412.

l'exécution (...)»¹²⁸. Dans la catégorie « sécurité », figure la sous-catégorie « harcèlement et intimidation » qui interdit de « faire preuve de malveillance ciblée en appelant à l'automutilation ou au suicide d'une personne en particulier ou d'un groupe de personnes »¹²⁹.

Une technique largement utilisée par les plateformes afin de réguler le contenu indésirable est le signalement¹³⁰. Sur Facebook par exemple, un utilisateur peut signaler un profil, un article, une publication ou une photo qu'il juge inapproprié¹³¹. Le réseau social examinera alors le signalement et, si la publication ou le profil incriminés sont contraires aux « standards de communauté », prendra des mesures envers le contenu et/ou l'utilisateur. Il est alors possible que les plateformes décident de retirer certains contenus jugés contraires à leurs règles d'autorégulation. Si l'individu dont la publication ou le compte ont été signalés pense qu'une erreur a été commise à son encontre, il peut demander qu'une deuxième analyse soit effectuée¹³². Il est donc possible de faire appel des décisions de retrait sur le contenu individuel.

Au sujet de l'usage de pseudonymes, les règles diffèrent selon les plateformes. Sur Facebook on peut lire, dans la rubrique « Noms autorisés sur Facebook », que le nom du profil doit être celui qui correspond au nom utilisé dans la vie courante, à savoir celui figurant sur la pièce d'identité¹³³. En revanche, sur le réseau social X (nouveau nom de « Twitter » depuis le 24 juillet 2023), on peut lire dans l'article « Comment modifier votre nom d'utilisateur Twitter ? » : « Votre nom d'affichage, ou plus simplement votre nom, est un identifiant personnel sur Twitter, distinct de votre nom d'utilisateur. Il peut s'agir d'un nom ludique, du nom d'une entreprise ou d'un vrai nom. Il est affiché à côté de votre nom d'utilisateur. »¹³⁴

¹²⁸Facebook, « Standards de la communauté Facebook », disponible sur <https://transparency.fb.com/fr-fr/policies/community-standards>, consulté le 24 juillet 2023.

¹²⁹Facebook, « Harcèlement et intimidation », disponible sur <https://transparency.fb.com/fr-fr/policies/community-standards/bullying-harassment/>, consulté le 24 juillet 2023.

¹³⁰A. ADAM, *op. cit.*, p. 88.

¹³¹Facebook, « Signaler quelque chose », disponible sur <https://www.facebook.com/help/263149623790594>, consulté le 13 juillet 2023.

¹³²M. BICKERT, « Standards de la Communauté : Facebook publie ses directives internes et élargit son processus de recours aux contenus individuels », disponible sur <https://about.fb.com/fr/news/2018/04/standards-de-la-communaute-facebook-publie-ses-directives-interne-et-elargit-son-processus-de-recours-aux-contenus-individuels/>, consulté le 8 juillet 2023.

¹³³Facebook, « Noms autorisés », disponible sur <https://www.facebook.com/help/112146705538576>, consulté le 13 juillet 2023.

¹³⁴X, « Comment modifier votre profil twitter », disponible sur <https://help.twitter.com/fr/managing-your-account/change-twitter-handle>, consulté le 5 août 2023.

Section 2 : Point de vue critique

À travers les règles d'autorégulation, les plateformes des réseaux sociaux endossent d'une part le rôle du législateur, en définissant les comportements à adopter, et d'autre part le rôle du juge, en analysant et déterminant la légitimité d'un contenu au cas par cas¹³⁵.

Toutefois, selon P.-F. DOCQUIR, certaines décisions individuelles de retrait de contenu peuvent être disproportionnées et incompatibles avec le droit à la liberté d'expression¹³⁶. L'auteur illustre ses propos par l'exemple d'une vidéo en direct ou publiée sur Facebook par le témoin d'une scène de violence lors d'un contrôle policier au cours duquel la personne contrôlée décède. D'après les règles de la communauté, c'est une scène de violence. Selon l'auteur, « la vidéo contrevient aux règles alors que cette vidéo pourrait être protégée par le droit de liberté d'expression en tant que contribution à un débat d'intérêt général »¹³⁷. Ensuite, une restriction à la liberté d'expression nécessiterait de remplir la condition de la base légale. Comme nous l'avons analysé précédemment, le droit à la liberté d'expression peut être restreint si l'ingérence est prévue par la loi. Selon P.-F. DOCQUIR, cette condition ne serait pas remplie. Il indique qu'une « atteinte doit reposer sur une règle qui doit être à la fois accessible et suffisamment précise pour permettre à un individu, au besoin s'entourant d'un conseil professionnel, de prévoir les conséquences de ses actes »¹³⁸. Certes, ces conditions générales sont accessibles à tous, mais l'on peut se questionner sur le caractère « suffisamment précis pour permettre à un individu de prévoir les conséquences de ces actes »¹³⁹.

Par ailleurs, certains auteurs critiquent la procédure de signalement. Ils remettent en question la légitimité des plateformes à décider du comportement à adopter. A. ADAM se questionne : « En quelle qualité et dotées de quelle légitimité ces entreprises privées sont-elles aptes à décider de ce qui est ou non acceptable dans un espace public et qui mérite ou non de rester dans l'anonymat ? »¹⁴⁰

¹³⁵N. ELKIN-KOREN et M. PEREL, « Guardian the Guardians: Content Moderation by Online Intermediaries and the Rule of Law », in *The Oxford Handbook of Online Intermediary Liability*, Oxford University Press, Oxford, 2020, p. 669.

¹³⁶P.-F. DOCQUIR, « Chapitre 2. - La confrontation entre droits fondamentaux et puissances privées vue à travers le prisme de la liberté d'expression », in *L'Europe des droits de l'homme à l'heure d'Internet*, Bruxelles, Bruylant, 2019, p. 85.

¹³⁷*Ibid.*

¹³⁸P.-F. DOCQUIR, *op.cit.*, p. 84.

¹³⁹*Ibid.*

¹⁴⁰A. ADAM, *op. cit.*, p. 90.

En définitive, les plateformes réagissent lorsqu'un comportement, interdit par les mesures d'autorégulation qu'elles ont édictées, a été signalé par un autre utilisateur. À ce moment-là, le réseau social prend des mesures, variant selon la gravité de l'infraction.

En matière de pseudonyme, la politique des plateformes diffère. Certaines l'autorisent explicitement, d'autres non. Cependant, dans les deux cas, les plateformes ne semblent pas prévoir concrètement de procédures permettant de révéler l'identité des individus. D'après O. BOGAERT, ce n'est pas réalisable de demander à Facebook de vérifier les comptes étant donné le grand nombre d'utilisateurs¹⁴¹.

Il conviendra dès lors d'analyser les mesures de corégulation/coopération¹⁴² entre les prestataires et les autorités judiciaires¹⁴³.

Chapitre 2 : Obligation d'information des prestataires de services de la société de l'information (Directive 2000/31/CE)

Section 1 : Base juridique

L'obligation d'information des prestataires de services de la société de l'information découle de la Directive 2000/31/CE¹⁴⁴ 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 (ci-après : « Directive commerce électronique » ; « Directive e-commerce »). La Directive a été transposée en droit belge par la loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information (ci-après : « LSSI »)¹⁴⁵. Par la suite, le Code de droit économique a été adopté et les dispositions ont été intégrées dans le Chapitre 6 intitulé « Responsabilité des prestataires intermédiaires », sous les articles XII.17 à 20¹⁴⁶.

¹⁴¹Voy. Annexe, questions 8 et 8bis de la retranscription de l'entretien avec Monsieur OLIVIER BOGAERT, membre de la *Federal Computer Crime Unit* (FCCU), le 31 juillet 2023.

¹⁴²Y. POULLET, « La lutte contre le racisme et la xénophobie sur internet », *op. cit.*, p. 411.

¹⁴³C. CASTETS-RENARD, *op. cit.*, p. 162.

¹⁴⁴Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information et notamment du commerce électronique dans le marché intérieur (« Directive sur le commerce électronique »), *J.O.C.E.* no L 178 du 17 juillet 2000.

¹⁴⁵Loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information, *M.B.*, 17 mars 2003.

¹⁴⁶Code de droit économique, art. XII.17 à 20.

À l'époque de l'adoption de cette Directive, le législateur européen voulait trouver un équilibre entre d'une part l'intention de ne pas faire peser une responsabilité trop lourde sur les intermédiaires techniques, qui n'ont pas connaissance des contenus qu'ils transportent et stockent, et d'autre part le besoin de protéger d'éventuelles victimes et de lutter efficacement contre les actes illicites.

La Directive établit aussi un principe de non-responsabilité des prestataires de services de la société de l'information, que nous analyserons ultérieurement. Cependant, en contrepartie à ce régime favorable, le législateur a prévu une obligation d'information à charge de ces prestataires¹⁴⁷. Cette obligation est reprise à l'article 15, §2 de la Directive, transposé à l'article 21, §2 de la LSSI et par la suite déplacé à l'article du XII.20, §2 du Code de droit économique.

Section 2 : Champ d'application

A travers la disposition de la Directive, les États membres ont la possibilité de mettre en place une obligation d'informer promptement les autorités publiques compétentes en cas d'activité manifestement illicite alléguée exercée par certains utilisateurs de leurs services, ou de communiquer aux autorités compétentes, à leur demande, les informations permettant d'identifier les destinataires de leurs services¹⁴⁸.

Cette obligation s'impose aux prestataires de services de la société de l'information, qui se répartissent en trois catégories à savoir les fournisseurs d'accès à internet (ci-après : « FAI »), les prestataires temporaires de stockage, et les prestataires d'hébergement¹⁴⁹.

Sous-section 1 : Caractère manifestement illicite

Pour nous aider à cerner la nature des actes qualifiés de « manifestement illicites », l'auteur R. HARDOUIN indique qu'il s'agit de contenus violant l'intérêt général, tels que ceux faisant l'apologie des crimes contre l'humanité ou incitant à la haine raciale, plutôt que ceux touchant aux intérêts privés, tels les droits de propriété intellectuelle¹⁵⁰.

¹⁴⁷E. MONTERO, *op. cit.*, p. 386.

¹⁴⁸Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 précitée, art. 15, §2.

¹⁴⁹C. CASTETS-RENARD, *op. cit.*, p. 156.

¹⁵⁰R. HARDOUIN, « La jurisprudence, les textes et la responsabilité des hébergeurs », *R.L.D.I.*, 2008/39, p. 68.

Concernant les actes entraînant une atteinte à la propriété intellectuelle ou à la vie privée, Z. KARAMBIRI estime, quant à lui, qu'il revient au juge de déterminer si le délit est constitué ou pas, et non pas au prestataire de service¹⁵¹.

Sous-section 2 : Informations permettant d'identifier les destinataires

Cette disposition implique l'obligation pour le prestataire de communiquer aux autorités des informations permettant d'identifier les destinataires. Se pose dès lors la question de la nature de ces données identifiantes.

Dans une affaire de la Cour d'appel de Paris, Benetton c. Google Inc.¹⁵², les autorités françaises avaient demandé à Google de leur fournir lesdites données. La société a fourni l'adresse électronique, l'adresse IP, et l'historique des connexions. L'adresse IP, diminutif de « Internet Protocole », est « une représentation numérique de l'endroit où un appareil est connecté à Internet »¹⁵³. Elle est assignée par votre fournisseur d'accès à internet¹⁵⁴ pour chaque appareil connecté à internet¹⁵⁵. Google n'a cependant pas donné le nom, le prénom et l'adresse, parce que la société n'était pas en possession de ces informations. Les informations données ont été jugées non pertinentes en ce qu'elles ne permettaient pas d'identifier les auteurs d'une infraction. Toutefois, Google maintenait qu'il n'y avait pas de définition légale concernant ces données dites « identifiantes ». La juridiction a estimé que Google était responsable en raison du non-respect de l'obligation tirée de l'article 15 de la Directive 2000/31/CE.

Par contre, dans une affaire du Tribunal de grande instance de Paris de 2007¹⁵⁶, le tribunal avait affirmé que l'adresse IP était une donnée satisfaisante. Le tribunal indique : « Il n'est pas contestable que le prestataire ayant fourni l'accès internet est en mesure de communiquer les coordonnées sous lesquelles il a souscrit son abonnement. »¹⁵⁷

¹⁵¹Z. KARAMBIRI, *op. cit.*, p. 42.

¹⁵²C.A. Paris, 14^e ch., sect. A, 12 décembre 2007, Google Inc / Benetton, Bencom.

¹⁵³A. PATRIZIO, « Qu'est-ce qu'une adresse IP? », disponible sur <https://www.avast.com/fr-fr/c-what-is-an-ip-address>, consulté le 31 juillet 2023.

¹⁵⁴M. UNTERSINGER, *op. cit.*, p. 58.

¹⁵⁵F. DONNAT, *Droit européen de l'internet : Réseaux, données, services*, Paris, L.G.D.J., 2018, p. 20.

¹⁵⁶T.G.I. Paris (réf.), 29 octobre 2007.

¹⁵⁷T.G.I. Paris (réf.), 29 octobre 2007.

Nous voyons, à travers ces deux illustrations, qu'il n'existe pas de consensus clair au sujet de la nature des données pouvant identifier un individu, ce qui ne manque pas de créer de l'insécurité juridique.

Sous-section 3 : Compétences des autorités judiciaires

L'article 15, §2 de la Directive sur le commerce électronique, correspondant à l'article XII.20, §2 du Code de droit économique, indique par ailleurs que seules les autorités judiciaires sont compétentes pour demander les données identifiantes des utilisateurs. Les victimes elles-mêmes ne peuvent accéder à l'identité de l'auteur d'une infraction ; il n'existe pas de droit subjectif accordé aux individus à cet égard¹⁵⁸. H. JACQUEMIN souligne que l'article 21, §2 de la LSSI (maintenant l'article XII.20, §2 du Code de droit économique) ne confère pas, à toute personne estimant être victime de propos calomnieux ou diffamatoires, un droit subjectif pour obtenir des autorités compétentes les moyens de poursuivre civilement les auteurs¹⁵⁹. La victime ne peut donc pas obtenir des autorités judiciaires qu'elles ordonnent au prestataire de lui communiquer les informations relatives à l'auteur¹⁶⁰. Dans un arrêt de la Cour de cassation belge du 16 juin 2011, la Cour confirme que cette disposition « ne crée pas de prérogative pour la victime, ni envers le prestataire intermédiaire, ni envers l'autorité judiciaire ou administrative »¹⁶¹.

Selon H. JACQUEMIN, il est inquiétant de voir certains individus profiter de cet anonymat relatif pour émettre des propos diffamatoires ou calomnieux sans risquer d'engager leur responsabilité civile¹⁶². Cette position a été confirmée par le juge des référés du Tribunal de première instance de Bruxelles dans une ordonnance du 4 juillet 2022¹⁶³. Dans cette affaire, la demanderesse sollicitait du juge des référés qu'il ordonne à Twitter de lui communiquer les données d'identification d'utilisateurs. Le juge a indiqué qu'« il était dans l'impossibilité de faire droit à sa demande en raison d'un « choix politique » et d'une mise en balance entre multiples intérêts et droits fondamentaux »¹⁶⁴ et que ce n'était pas à lui, en tant que juge, de modifier ou

¹⁵⁸Cass., 16 juin 2011, *R.D.T.I.*, 2012, p. 69.

¹⁵⁹H. JACQUEMIN, « Qui peut obtenir les informations permettant de rechercher et de poursuivre les auteurs d'infractions commises sur les réseaux ? », note sous Cass. (1re ch.), 16 juin 2011. *R.D.T.I.*, (47), p. 77.

¹⁶⁰E. CORNU et B. DOCQUIR, « L'usage des réseaux sociaux : entre droits intellectuels, liberté d'expression et vie privée », in *Les réseaux sociaux et le droit* (sous la dir. de M. SALMON), Bruxelles, Larcier, 2014, p. 121.

¹⁶¹Cass., 16 juin 2011, *R.D.T.I.*, 2012, p. 69.

¹⁶²H. JACQUEMIN, *op.cit.*, p. 79.

¹⁶³Civ. Bruxelles fr. (réf), 4 juillet 2022, R.G., n°2022/24/C.

¹⁶⁴Civ. Bruxelles fr. (réf), 4 juillet 2022, R.G., n°2022/24/C.

contourner cela¹⁶⁵. Selon A. ADAM, il serait nécessaire de revoir cette mise en balance et d'ouvrir la voie civile aux victimes de comportements illicites en leur permettant d'obtenir l'identification d'auteurs anonymes¹⁶⁶. Effectivement, sans l'identification de l'auteur, la victime n'a pas accès à un recours effectif permettant de le poursuivre dans le cadre d'une procédure civile¹⁶⁷.

Pour remédier à cette situation, H. JACQUEMIN suggère d'amender l'article 21 §1, al. 2 de la loi du 11 mars 2003 (maintenant reprise à l'article XII.20 du Code de droit économique) pour ainsi permettre aux victimes d'obtenir les informations nécessaires, tout en mettant des garanties en place telles que l'intervention de l'autorité judiciaire¹⁶⁸. Il propose de modifier la disposition comme suit : « Sans préjudice d'autres dispositions légales ou réglementaires, les mêmes prestataires sont tenus de communiquer aux autorités judiciaires ou administratives compétentes, à leur demande, toutes les informations dont ils disposent et utiles à la recherche et à la constatation des infractions commises par leur intermédiaire. Indépendamment de poursuites pénales ou administratives, les autorités judiciaires compétentes peuvent également ordonner aux prestataires de communiquer les mêmes informations aux personnes victimes de ces infractions s'il existe des indices sérieux démontrant que les éléments constitutifs de ces infractions sont réunis et pour autant que les droits de la victime ne puissent pas être préservés par la mise en œuvre de mesures moins attentatoires à la vie privée de l'auteur de l'acte. »¹⁶⁹ Bien que cette proposition donne plus de compétence à la victime pour agir, l'auteure A. ADAM estime qu'elle ne donne pas compétence au juge civil pour opérer cet examen¹⁷⁰. Cela aurait pour conséquence de contraindre les victimes à activer la voie pénale, même lorsque ces dernières souhaiteraient uniquement obtenir réparation du dommage.

¹⁶⁵Civ. Bruxelles fr. (réf), 4 juillet 2022, R.G., n°2022/24/C.

¹⁶⁶A. ADAM, *op. cit.*, p. 95.

¹⁶⁷*Ibid.*

¹⁶⁸H. JACQUEMIN, *op.cit.*, p. 79.

¹⁶⁹H. JACQUEMIN, *op.cit.*, pp. 80-81.

¹⁷⁰A. ADAM, *op. cit.*, p. 101.

Section 3 : Principe de non-responsabilité pour les actes des utilisateurs

Comme évoqué précédemment, cette obligation d'information des prestataires de services a été mise en place pour contrebalancer le régime favorable octroyé aux plateformes, à savoir le principe de non-responsabilité. Il est un fait que les prestataires de services ne commettent pas eux-mêmes les infractions, étant donné qu'ils sont considérés comme des intermédiaires techniques. Ils ne peuvent dès lors pas être tenus responsables du contenu qu'ils hébergent.

La Directive 2000/31/CE prévoit de ce fait un principe de non-responsabilité pour les prestataires de services de la société de l'information pour les actes commis par les utilisateurs¹⁷¹. Selon ce principe, les trois catégories de prestataires techniques destinataires de la norme ne seront pas tenus responsables du fait des contenus émanant de tiers, pour autant qu'ils respectent les conditions prescrites par la loi¹⁷².

Lorsque la Directive a été adoptée, ces prestataires avaient en commun un rôle purement technique. Avec l'apparition du web 2.0 ces dernières années, leur rôle a fortement évolué et s'est diversifié¹⁷³. Le considérant 42 de la Directive précise toutefois que le principe de non-responsabilité couvre uniquement les situations où l'activité du prestataire revêt un caractère purement technique, automatique et passif¹⁷⁴.

Sous-section 1 : Conditions pour bénéficier de l'exemption de responsabilité

Le principe de non-responsabilité des fournisseurs d'accès à internet se trouve repris à l'article 12, §1 de la Directive e-commerce, transposé à l'article XII.17 du Code de droit économique. Cette disposition établit les conditions pour pouvoir bénéficier du régime d'exemption de responsabilité pour les fournisseurs d'accès à internet qui transmettent des informations sur un réseau de communication. Selon cet article, le prestataire de services n'est pas tenu responsable des informations transmises s'il respecte les conditions suivantes : « a) il n'est pas à l'origine de la transmission; b) il ne sélectionne pas le destinataire de la transmission; c) il ne sélectionne, ni ne modifie, les informations faisant l'objet de la transmission »¹⁷⁵. Selon cette disposition,

¹⁷¹Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 précitée, art. 12, 13, 14.

¹⁷²F. GEORGE et J. HUBIN, *op. cit.*, p. 209.

¹⁷³F. GEORGE et J. HUBIN, *op. cit.*, p. 226.

¹⁷⁴Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 précitée, considérant 42.

¹⁷⁵Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 précitée, art. 12, §1.

les FAI sont exemptés du régime de responsabilité s'ils ne sont intervenus aucunement dans la transmission.

En ce qui concerne les hébergeurs, l'article 14, §1 de la directive, transposé à l'article XII.19 du Code de droit économique, précise que le prestataire de services n'est pas responsable des informations stockées à la demande d'un destinataire du service à condition que : « a) le prestataire n'ait pas effectivement connaissance de l'activité ou de l'information illicites et, en ce qui concerne une demande en dommages et intérêts, n'ait pas connaissance de faits ou de circonstances selon lesquels l'activité ou l'information illicite est apparente ou b) le prestataire, dès le moment où il a de telles connaissances, agisse promptement pour retirer les informations ou rendre l'accès à celles-ci impossible »¹⁷⁶.

En définitive, les prestataires de services bénéficient en principe du régime de non-responsabilité. Cependant, ils peuvent voir leur responsabilité engagée lorsqu'ils ne respectent pas les obligations qui leur incombent¹⁷⁷.

Sous-section 2 : Responsabilité en cas de manquement à une obligation

Malgré cette règle de non-responsabilité de principe, la Directive prévoit des hypothèses permettant néanmoins d'engager la responsabilité de ces prestataires techniques¹⁷⁸. On ne peut *a priori* pas imputer la responsabilité d'un prestataire qui n'est pas à l'origine des contenus illicites postés dans son réseau et qui ne contrôle pas ceux-ci. En revanche, s'il en est informé, il doit agir rapidement pour ne plus en permettre l'accès¹⁷⁹. En effet, en interprétant les conditions des articles 12 et 14 de la Directive *a contrario*, la responsabilité des prestataires techniques pourrait être engagée si le prestataire a « effectivement connaissance de l'activité ou de l'information illicites », ou « en ce qui concerne une demande en dommages et intérêts », s'il avait « connaissance de faits ou de circonstances selon lesquels l'activité ou l'information illicite est apparente », ou encore si « dès le moment où il a de telles connaissances il n'aurait pas agi promptement pour retirer les informations ou rendre l'accès à celles-ci impossible »¹⁸⁰.

¹⁷⁶Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 précitée, art.14, §1.

¹⁷⁷Z. KARAMBIRI, *op. cit.*, p. 41.

¹⁷⁸E. DERIEUX, A. GRANCHET, *op. cit.*, p. 109.

¹⁷⁹C. CASTETS-RENARD, *op. cit.*, p. 160.

¹⁸⁰Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 précitée, art. 12 et 14 *a contrario*.

Section 4 : Point de vue critique

Concernant l'obligation d'information de l'article XII. 20, §2 du Code de droit économique, certains auteurs critiquent le fait qu'aucune procédure spécifique n'a été mise en place en droit belge pour fixer les conditions et formes de cette notification ni pour imposer un délai endéans lequel la réaction du réseau social est attendue¹⁸¹.

Par ailleurs, certains auteurs ont apporté des critiques, positives comme négatives, au principe de non-responsabilité des intermédiaires.

Tout d'abord, certains sont favorables à ce régime d'exemption de responsabilité, car selon eux imposer un régime de responsabilité trop strict aux prestataires aurait comme conséquence une augmentation du contrôle du contenu¹⁸². Selon C. CASTETS-RENARD, les hébergeurs auraient intérêt à engager une démarche proactive pour supprimer un contenu ambigu afin d'éviter que leur responsabilité ne soit engagée¹⁸³. Cela pourrait mettre à mal le droit à la liberté d'expression des utilisateurs¹⁸⁴.

À l'opposé, certains auteurs regrettent la mise en place de ce régime, car ils affirment que, même si ce ne sont pas les intermédiaires qui posent directement les actes problématiques, ils les rendent possibles, d'une certaine manière, à travers leur rôle d'intermédiaires¹⁸⁵. En outre, contrairement à l'auteur de l'infraction qui peut être difficilement identifiable ou insolvable, les plateformes présentent l'avantage d'être facilement identifiables, localisables et solvables¹⁸⁶.

Enfin, une critique générale est liée au caractère dépassé de la directive, adoptée il y a plus de 23 ans. Entre 2000 et 2023, les réalités numériques ont bien changé. À l'époque, l'adoption de

¹⁸¹A. ADAM, *op. cit.*, p. 93.

¹⁸²C. CASTETS-RENARD, *op. cit.*, p. 172; D. KELLER, « Internet Platforms: Observations on Speech, Danger and Money », *Hoover institution's Aegis Paper Series*, 2018, n°1807.

¹⁸³C. CASTETS-RENARD, *op. cit.*, p. 172.

¹⁸⁴A. LUCAS, « La responsabilité civile des acteurs de l'Internet », *A&M*, 2001/1, p. 46. ; A. MICHEL, « La régulation de la modération des contenus en ligne, une affaire de droits humains ? », *Rev. Trim. D.H.*, 2023/133, p. 41.

¹⁸⁵Z. KARAMBIRI, *op. cit.*, p. 32. ; M. KEUP, « Obtenir une mesure de blocage d'un site Internet contre un fournisseur d'accès à Internet : état des lieux », *R.D.C.-T.B.H.*, 2019/6, p. 714. ; T. LEONARD, *op. cit.*, p. 127.

¹⁸⁶F. GEORGE et J. HUBIN, *op. cit.*, p. 208.

ces règles, harmonisant les exonérations de responsabilités¹⁸⁷, avait pour objectif principal de ne pas compromettre le développement d'internet et du commerce électronique¹⁸⁸. Les divergences des législations nationales d'alors pouvaient en effet constituer des obstacles aux échanges, empêcher le développement des services transfrontaliers et produire des distorsions de concurrence¹⁸⁹. D'autre part, ce régime a été conçu à une époque où les plateformes n'avaient ni les caractéristiques ni la taille qu'elles ont aujourd'hui¹⁹⁰. Le contexte du web 2.0 diffère considérablement de celui du web 1.0 qui existait au moment de l'entrée en vigueur de la Directive. Le jugeant trop ancien et décalé par rapport aux évolutions¹⁹¹, certains auteurs ont appelé à une réforme du système de responsabilité des intermédiaires, afin de l'ajuster aux évolutions technologiques¹⁹².

Section 5 : Digital Services Act (DSA)

Soucieux précisément d'adapter le régime de responsabilité aux enjeux actuels, le législateur européen a adopté le Règlement (UE) 2022/2065 relatif à un marché unique des services numériques, plus communément appelé le Digital Service Act¹⁹³ (ci-après « DSA »). Le DSA, modifie la Directive 2000/31 et sera d'application à partir du 17 février 2024¹⁹⁴.

L'objectif du DSA est double. D'une part, il entend harmoniser les règles applicables aux prestataires de services intermédiaires, tout en ne freinant pas l'innovation numérique¹⁹⁵. Le législateur européen était en effet inquiet de voir plusieurs initiatives prises individuellement par les États membres. D'autre part, le Règlement veut également encadrer et réduire le pouvoir des grandes plateformes numériques¹⁹⁶.

¹⁸⁷Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions, « Les plateformes en ligne et le marché unique numérique – Perspectives et défis pour l'Europe », COM (2016) 288 final.

¹⁸⁸C. CASTETS-RENARD, *op. cit.*, p. 154.

¹⁸⁹Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 précitée, considérant 40.

¹⁹⁰F. GEORGE et J. HUBIN, *op. cit.*, p. 218.; C. CASTETS-RENARD, *op. cit.*, p. 171.

¹⁹¹A. BLANDIN-OBERNESSER, « Digital Services Act et Digital Markets Act : un nouveau cadre européen pour la régulation des plateformes », in *La politique européenne du numérique* (sous la dir. de B. BERTRAND), 1^{re} édition, Bruxelles, Bruylant, 2022, p. 693.

¹⁹²E. MONTERO, *op. cit.*, p. 388.

¹⁹³Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la Directive 2000/31/CE (« Règlement sur les services numériques »), J.O.U.E., 27 octobre 2022, n° L 277.

¹⁹⁴Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 précité, art. 93.

¹⁹⁵R. TINIÈRE, « L'Union européenne et la régulation des plateformes en ligne – À la recherche de la voie du milieu », in *La politique européenne du numérique* (sous la dir. de B. BERTRAND), 1^{re} édition, Bruxelles, Bruylant, 2022, p. 704.

¹⁹⁶A. BLANDIN-OBERNESSER, *op. cit.*, p. 694.

Concrètement, la majorité des dispositions de la Directive e-commerce vont rester en vigueur et quelques dispositions vont être intégrées dans le DSA¹⁹⁷. C'est notamment le cas des articles 12 à 15 de la Directive 2000/31 concernant l'exemption de responsabilité qui figurent aux articles 4 à 8 du DSA¹⁹⁸.

Ce Règlement s'applique aux prestataires qui fournissent des services de simple transport, de mise en cache ou d'hébergement¹⁹⁹, établis ou résidant sur le territoire de l'Union européenne.

En matière de responsabilité des plateformes, le DSA prévoit, en son chapitre II, une exemption conditionnelle de responsabilité des fournisseurs de services intermédiaires. En passant de la Directive e-commerce au DSA, le régime de responsabilité des plateformes change d'un régime de responsabilité conditionnelle à un régime où la responsabilité dépend de l'organisation adoptée par l'entreprise par rapport à divers types de contenu²⁰⁰.

Le Règlement ajoute par ailleurs d'autres obligations à charge des prestataires, notamment des obligations de diligence visant à créer les conditions d'un environnement en ligne sûr et transparent. Ces obligations, figurant au chapitre III, sont reprises sous la forme d'un système graduel : « plus un service a d'utilisateurs, plus il a une responsabilité sociétale et donc d'obligations »²⁰¹. Il s'agit d'un axe majeur de ce nouvel instrument. Cette approche graduée prend en considération notamment la taille et les moyens du prestataire concerné²⁰². Par exemple, les « fournisseurs de plateformes en ligne » ont l'obligation de coopérer avec les autorités nationales à la suite d'injonctions²⁰³ ; l'obligation de désigner un représentant légal dans l'Union pour les fournisseurs qui ne sont pas établis dans un État membre²⁰⁴ ; l'obligation de fournir aux bénéficiaires du service un mécanisme de réclamation et de recours²⁰⁵ ainsi que

¹⁹⁷J. HOUDIK, « The e-Commerce Directive and its relation to the proposed Digital Services Act : is the European Union ready for a new digital age? », in *L'influence du droit européen en droit économique / Cabinet de curiosités pour un juriste passionné – Liber Amicorum Denis Philippe* (sous la dir. de A. STROWEL, G. MINNE), 1^e édition, Bruxelles, Larcier, 2022, p. 755.

¹⁹⁸P. CAMPOLINI, J. CABAY, M. BERWETTE, J. BIART et G. CROISANT, « Chronique de législation en droit privé (Deuxième partie) », *J.T.*, 2023/23, n° 6945, p. 373-381.

¹⁹⁹Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 précité, art. 3, g.

²⁰⁰M.-L. MONTAGNANI, « Intermediary Liability Regime in the Digital Single Market », in *Questions choisies de droit européen des affaires / Selected Issues in European Business Law* (sous la dir. de P. VAN CLEYNENBREUGEL et J. WILDEMEERSCH), 1^e édition, Bruxelles, Bruylant, 2023, p. 130.

²⁰¹P. CAMPOLINI, J. CABAY, M. BERWETTE, J. BIART et G. CROISANT, *op. cit.*, p. 373-381.

²⁰²A. MICHEL, *op. cit.*, p. 43.

²⁰³Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 précité, art. 9 et 10.

²⁰⁴Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 précité, art. 13.

²⁰⁵Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 précité, art. 20.

de règlement extrajudiciaire de litiges²⁰⁶, etc. Les « fournisseurs de très grandes plateformes en ligne » ont d'autres obligations, dont celle de partager des données avec les autorités et les chercheurs²⁰⁷.

En outre, une analyse et une évaluation avec diligence de tout risque systémique découlant de la conception, y compris des systèmes algorithmiques, du fonctionnement et de l'utilisation faite de leurs services dans l'Union²⁰⁸ est imposée aux plateformes par l'article 26 du DSA²⁰⁹.

Le Règlement identifie les risques mais ne règle pas le fond. Il laisse aux États membres le soin de définir les règles concrètes²¹⁰.

Étant donné que cet instrument juridique, réformant la Directive e-commerce, n'est pas encore d'application actuellement, il faudra attendre les prochaines années pour l'évaluer et voir s'il répond ou non aux critiques adressées à la Directive 2000/31/CE.

Chapitre 3 : Obligation de collaboration de l'opérateur d'un réseau de communication ou d'un fournisseur de services de communication électronique (Article 46bis du Code d'instruction criminel)

Section 1 : Base juridique

L'obligation de collaboration de l'opérateur d'un réseau de communication ou d'un fournisseur de services de communication électronique se trouve à l'article 46bis du Code d'instruction criminel.

Cette disposition a connu une importante modification avec la loi du 25 décembre 2016²¹¹ portant des modifications diverses au Code d'instruction criminel et au Code pénal.

²⁰⁶Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 précité, art. 21.

²⁰⁷Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 précité, art. 40.

²⁰⁸E. DEBIES, « Comment lutter contre la désinformation sans porter atteinte aux droits fondamentaux et en particulier la protection des données : la recherche d'équilibre opérée par l'Autorité de protection des données (APD) belge dans l'affaire des messages Twitter à propos de l'affaire Benalla – Regard d'une juriste française », *R.D.T.I.*, 2022/2, pp. 100-101.

²⁰⁹Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 précité, art. 26.

²¹⁰A. BLANDIN-OBERNESSER, *op. cit.*, p. 694.

²¹¹Loi 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

Les travaux parlementaires indiquent que la loi a pour objectif de « mieux outiller les autorités judiciaires pour lutter contre la criminalité dans la société de l'information »²¹², raison pour laquelle la loi s'applique potentiellement à n'importe quelle infraction « pourvu qu'à un moment donné un système informatique ait été utilisé »²¹³.

Parmi les nombreux changements apportés par la loi du 25 décembre 2016, on retrouve la recherche non-secrète et la recherche secrète dans un système informatique, la conservation rapide de données informatiques, le contrôle visuel discret, les infiltrations sur internet, l'obligation de collaboration des fournisseurs de services, la banque de données à empreinte vocale, etc. La modification qui retient particulièrement l'attention dans le cadre de ce mémoire est l'obligation de collaboration des fournisseurs de services, notamment l'accès aux données d'identification qui s'avère indispensable pour de nombreuses enquêtes pénales²¹⁴.

Section 2 : Champ d'application

La disposition prévoit la possibilité pour le procureur du Roi et/ou le juge d'instruction de requérir, de l'opérateur d'un réseau de communication ou du fournisseur d'un service de communication électronique, l'identité et les coordonnées de l'abonné ou de l'utilisateur habituel d'un service de télécommunication²¹⁵, ainsi que les moyens de communication auxquels une personne déterminée est abonnée ou qu'elle utilise de manière habituelle²¹⁶.

Sous-section 1 : Arrêt Yahoo de la Cour de cassation

L'arrêt Yahoo de la Cour de cassation a permis de clarifier le champ d'application de cette procédure de collaboration. Pendant plus de sept ans, de 2007 à 2015, cette affaire a fait couler beaucoup d'encre en Belgique. Elle a par ailleurs entraîné l'adoption de la loi du 25 décembre 2016 précitée²¹⁷.

communications électroniques et les télécommunications et créant une banque de données des empreintes vocale, M.B., 17 janvier 2017.

²¹²Projet 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, *Doc. parl.*, Ch. repr., sess. ord., 2015-2016, n°54-1966/1, p.7.

²¹³V. FRANSSEN et O. LEROUX, *op. cit.*, p. 134.

²¹⁴V. FRANSSEN et O. LEROUX, *op. cit.*, p. 196.

²¹⁵C.i.cr, art. 46bis, § 1er, al. 1^{er}, 1^{er} tiret.

²¹⁶C.i.cr, art. 46bis, § 1er, al. 1^{er}, 2^e tiret.

²¹⁷Loi du 25 décembre 2016 précitée.

Concernant les faits, le procureur du Roi de Termonde ouvre, en 2007, une enquête contre des individus inconnus accusés d'escroquerie. Les suspects avaient utilisé plusieurs adresses mail Yahoo afin de commettre les infractions qui leur sont reprochées. Dans le besoin d'identifier les suspects, le procureur du Roi demande à l'entreprise américaine Yahoo de lui fournir des données d'identification des suspects, et ce sur base de l'article 46bis du C.i.cr.. Comme évoqué ci-dessus, cet article donne le pouvoir au procureur du Roi de solliciter le concours d'un opérateur de réseau de communication électronique ou d'un fournisseur de services de communication électronique. Cela lui permet d'obtenir l'identité du titulaire ou de l'utilisateur d'une adresse IP à un moment précis ainsi que les éléments d'identification propres à l'utilisateur.

L'entreprise refuse de lui fournir ces données ; ne possédant pas de siège sur le territoire belge, elle estime ne pas être soumise à la loi belge. Face à ce refus, le ministère public assigne Yahoo devant le tribunal correctionnel de Termonde, qui la condamne en 2009. L'argument du tribunal est le suivant : « Malgré qu'il s'agisse d'une entreprise américaine, elle constitue un fournisseur de services de communications électroniques présent de manière virtuelle et économique en Belgique et donc cette dernière doit être considérée comme judiciairement présente sur le territoire belge. »²¹⁸

Après cette condamnation, la société Yahoo décide d'interjeter appel devant la Cour d'appel de Gand. La Cour réforme le jugement du Tribunal correctionnel de Termonde par un arrêt du 30 juin 2010²¹⁹. Dans cet arrêt, la Cour acquitte Yahoo estimant que l'entreprise n'entre pas dans les notions d'opérateur et de fournisseur de services au sens de la loi du 13 juin 2005.

À la suite de cet arrêt, un pourvoi en cassation est introduit. La Cour de cassation décide de casser l'arrêt de la Cour d'appel de Gand et de renvoyer l'affaire devant la juridiction du second degré de Bruxelles²²⁰. Par un arrêt du 12 octobre 2011, la Cour d'appel de Bruxelles estime que le ministère public ne disposait pas du pouvoir juridictionnel pour exercer ses fonctions extra territorialement et donc que Yahoo n'avait pas manqué à ses obligations²²¹. Suite à cet arrêt, un nouveau pourvoi en cassation est introduit par le procureur général. Par un arrêt rendu le 4

²¹⁸Corr. Flandre orientale (div. Termonde), 2 mars 2009, *T. Strafr.*, 2009/2, p. 116.

²¹⁹Gand (3^e ch.), 30 juin 2010, *T. Strafr.*, 2011/22, p. 132.

²²⁰Cass. (2^e ch.), 18 janvier 2011, R.G. n° P.10.1347.N.

²²¹Bruxelles (13^e ch.), 12 octobre 2011, *A&M*, 2012/2-3, pp. 238 et 239.

septembre 2012, la Cour de cassation casse l'arrêt de la Cour d'appel de Bruxelles, validant l'extension territoriale de l'action des autorités belges²²². L'affaire est dès lors renvoyée devant la Cour d'appel d'Anvers, qui confirmera par un arrêt du 20 novembre 2013 le jugement du tribunal correctionnel de Termonde du 2 mars 2009²²³. Yahoo décide à son tour d'introduire un pourvoi devant la Cour de cassation. La Cour de cassation rend l'arrêt qui met fin à cette « saga » le 1 décembre 2015²²⁴, dans lequel elle considère que le procureur du Roi peut demander directement à des fournisseurs de services étrangers de collaborer étant donné que leurs activités économiques sont activement destinées à des consommateurs belges²²⁵.

Sous-section 2 : Champ d'application personnel

Avec ses nombreux rebondissements, cette affaire a soulevé plusieurs questions juridiques permettant de clarifier le champ d'application de l'obligation de collaboration prévue à l'article 46bis du Code d'instruction criminelle, tel que modifié par la loi du 25 décembre 2016 qui entérine la jurisprudence Yahoo. C'est l'objet de la présente section.

Le champ d'application personnel était en discussion dans l'affaire Yahoo. D'un côté, l'entreprise Yahoo défendait qu'elle n'était pas tenue de collaborer avec les autorités judiciaires belges étant donné qu'elle n'était ni un opérateur d'un réseau de communication électronique, ni un fournisseur d'un service de communication électronique. Selon elle, il convenait d'interpréter ce terme au sens que lui donnait l'article 2 de la loi du 13 juin 2005 relative aux communications électroniques. Selon cet argument, Yahoo serait exclu du champ d'application personnel de la disposition, l'entreprise fournissant simplement une application logicielle qui permet aux utilisateurs d'un compte email Yahoo d'envoyer et de recevoir des messages électroniques à n'importe quel endroit au monde. De l'autre côté, le ministère public soutenait qu'il convenait d'interpréter cette notion bien plus largement sur base du principe de l'autonomie du droit pénal.

Cette interprétation au sens large l'a emporté dans un arrêt du 18 janvier 2011 de la Cour de cassation. La Cour y affirme que « l'article 46bis C.i.cr. ne se limite dès lors pas aux opérateurs d'un réseau de communications électroniques ou aux fournisseurs d'un service de

²²²Cass. (2^e ch.), 4 septembre 2012, *T. Strafr.*, 2012/6, p. 464.

²²³Anvers (12^e ch.), 20 novembre 2013, *T. Strafr.*, 2014/1, p. 73.

²²⁴Cass. (2^e ch.), 1^{er} décembre 2015, R.G. n° P.13.2082.N.

²²⁵Cass. (2^e ch.), 1^{er} décembre 2015, R.G. n° P.13.2082.N, p. 4.

communications électroniques qui sont aussi opérateurs au sens de la loi du 13 juin 2005 ou qui dispensent leurs services de communications électroniques 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 voie de réseaux de communications électroniques et la personne qui fournit un service consistant au moyen d'un réseau électronique peut aussi être un fournisseur d'un service de communications électroniques »²²⁶. À ce jour, aucune dérogation n'est prévue par le législateur sur ce point²²⁷.

En doctrine, les auteurs ne sont pas tous d'accord quant à l'interprétation de la Cour à ce sujet. Certains affirment que cette interprétation large est en conformité avec l'article 1 de la Convention de Budapest donnant une définition large à la notion de fournisseur de services et qu'une interprétation plus restrictive aurait rendu l'identification d'auteurs d'infractions utilisant des services comme Yahoo, Hotmail ou Gmail simplement impossible²²⁸. D'autres auteurs s'opposent à cette interprétation, estimant qu'elle va à l'encontre de la volonté du législateur²²⁹ et qu'elle constitue une interprétation analogique interdite au détriment des individus²³⁰. D'autres encore sont d'avis que cette interprétation octroierait un pouvoir d'appréciation important au juge du fond et qu'une interprétation législative est donc nécessaire²³¹.

Malgré ces désaccords, la jurisprudence Yahoo de la Cour de cassation a été utilisée par la suite dans une affaire Skype. Dans cette affaire, les autorités belges avaient demandé à l'entreprise Skype des données relatives au trafic de communications d'utilisateurs. L'entreprise avait refusé. La Cour d'appel d'Anvers²³² a estimé qu'au final il importait peu que l'entreprise possède ou non un siège social ou un siège d'exploitation en Belgique, étant donné que Skype fournissait des moyens techniques à des utilisateurs pouvant ainsi communiquer entre eux par le biais d'un réseau électronique et échanger des données une fois qu'ils se sont inscrits et leurs données vérifiées. La Cour d'appel a estimé que l'entreprise aurait dû prendre les mesures techniques et organisationnelles appropriées afin de pouvoir se conformer à l'obligation de

²²⁶Cass., 18 janvier 2011, N.C., 2011, p.76, §6.

²²⁷M. GIACOMETTI, « Chapitre 2 - La récolte transfrontière de preuves électroniques en droit belge », in *La récolte transfrontière de preuves électroniques dans le contexte européen*, 1^e édition, Bruxelles, Bruylant, 2023, p. 661.

²²⁸V. FRANSSSEN et O. LEROUX, *op. cit.*, p. 198.

²²⁹P. DE HERT, G. BOULET, « Yahoo ! moetmeewerken met Belgische procureur », *Juristenkrant*, 2012, n°253, p.8.

²³⁰N. VANDEZANDE, « Yahoo ! als operator of vertrekker », note sous Cass., 18 janvier 2011, A.M., 2011, p. 223.

²³¹C. FORGET, « La collecte de preuves informatiques en matière pénale », in *Pas de droit sans technologie*, (sous la dir. de J. FR. HERNOTTE et F. JONGEN), coll. CUP, Bruxelles, Larcier, 2015, p.267.

²³²Anvers, 15 novembre 2017, §5.1.2.1.

collaboration imposée par le législateur belge. Cette décision a par la suite été confirmée par la Cour de cassation en date du 19 février 2019²³³.

L'adoption de la loi du 25 décembre 2016 met fin au débat. Le législateur belge décide d'entériner la jurisprudence Yahoo en ce qu'il adopte l'interprétation large : « La catégorie de fournisseurs doit être interprétée au sens large du terme incluant tant les entreprises qui proposent du web service comme Yahoo, Hotmail, Gmail, que des services comme Facebook, Twitter, WhatsApp, Instagram, et tous les autres services qui entrent dans la nouvelle définition légale. »²³⁴

Sous-section 3 : Champ d'application territorial

La loi du 25 décembre 2016 a clarifié le champ d'application territorial.

Dans l'arrêt Yahoo, la question était de savoir si ces fournisseurs de services étrangers pouvaient être contraints à collaborer avec la justice belge sans passer par une requête d'entraide judiciaire. La Cour a jugé que Yahoo, en tant que fournisseur d'un service de messagerie électronique gratuit, était présent sur le territoire de la Belgique et se soumettait volontairement à la loi belge en ce qu'elle participait activement à la vie économique en Belgique. Dans son raisonnement, la Cour utilise les indices suivants : l'usage du nom de domaine (www.yahoo.be), l'usage de la langue locale, la publicité faite en fonction de la localisation des utilisateurs et son accessibilité en Belgique pour ses utilisateurs²³⁵ liée à une boîte de réclamations et à une ligne d'assistance téléphonique, par exemple²³⁶. En 2019, dans un autre arrêt, la Cour de cassation réaffirme sa jurisprudence antérieure en affirmant : « Tout opérateur ou fournisseur de services qui offre des services sur le territoire belge et cible activement le marché belge est tenu de collaborer avec les autorités belges, peu importe où se trouve son siège et peu importe s'il a une infrastructure en Belgique. »²³⁷

²³³Cass., 19 février 2019, R.G. P.17.1229.N, *Computerr.*, 2019, p. 277.

²³⁴Projet 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, *Doc. parl.*, Ch. repr., sess. ord., 2015-2016, n°54-1966/1, pp. 32 et s.

²³⁵Cass., 1^{er} décembre 2015, R.G., n°P.13.2082.N.

²³⁶K. DE SCHEPPER., « Cassatie bevestigt: Belgische gerecht kan rechtstreeks gegevens vorderen van Yahoo », *R.A.B.G.*, 2016/7, p. 489-493.

²³⁷Cass., 19 février 2019, R.G. n°P.17.1229. N.

Sous-section 4 : Champ d'application temporel

La loi du 25 décembre 2016 précise également le champ d'application temporel de l'article 46bis du Code d'instruction criminelle. Les opérateurs et fournisseurs de services doivent communiquer les données requises par le procureur du Roi « en temps réel », sauf si la réquisition précise un autre moment.

La notion de « temps réel » ne signifie pas « immédiatement »²³⁸ mais entend le temps nécessaire à l'exécution de la prestation sollicitée, selon les règles de l'art, sans interruption et en mettant en œuvre les moyens et le personnel adéquats²³⁹.

Sous-section 5 : Champ d'application matériel

Enfin, la loi clarifie le champ d'application matériel. La coopération des fournisseurs de services peut être requise à l'occasion de l'exécution de trois mesures d'enquête, dont la mesure visée par l'article 46bis C.i.cr., à savoir l'identification d'un abonné ou de l'utilisateur habituel d'un service de communication électronique ainsi que l'identification du moyen ou des services de communication électronique qu'il utilise²⁴⁰.

Section 4 : Point de vue critique

Selon M. GIACOMETTI, cette procédure peut être considérée comme avant-gardiste²⁴¹, tant sur le plan de l'efficacité que sur celui de l'étendue des pouvoirs d'investigation. Il s'agit en effet d'un véritable pas en avant en matière de procédure pénale octroyant des pouvoirs aux autorités judiciaires. C'est une procédure importante permettant de révéler l'identité d'un individu sur les réseaux sociaux. Avec cette disposition, les autorités judiciaires peuvent obliger les plateformes comme Facebook à collaborer avec elles, et ce notamment pour permettre d'accéder à l'identité d'un délinquant.

²³⁸Projet 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, *Doc. parl.*, Ch. repr., sess. ord., 2015-2016, n°54-1966/1, p. 34.

²³⁹A.R. du 9 janvier 2003 déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques, *M.B.*, 10 février 2003, art. 1, 3°.

²⁴⁰C.i.cr., art. 46bis, §1, al. 2.

²⁴¹M. GIACOMETTI, « Chapitre 2 - La récolte transfrontière de preuves électroniques en droit belge », *op. cit.*, p. 679.

En outre, la loi du 25 décembre 2016 ajoute des sanctions financières pouvant aller jusqu'à 30 000€²⁴², dans les cas où les plateformes refusent de coopérer. Il s'agit d'un élément incitatif important. Toutefois, M. GIACOMETTI estime que cette somme est dérisoire au regard de leur chiffre d'affaires²⁴³, qui s'élève, pour Facebook, à 28,580 milliards de dollars (dont 10,394 milliards de dollars de bénéfices) pour le second semestre 2021²⁴⁴.

Par ailleurs, certains critiquent cette procédure qui constituerait, selon eux, un « non-sens juridique » au regard du principe de territorialité²⁴⁵. En droit international, il existe en effet des principes de territorialité et d'égalité souveraine²⁴⁶ qui interdisent aux États d'exercer leur compétence procédurale en dehors de leurs frontières nationales à moins qu'il y ait eu une autorisation par « une règle permissive découlant du droit international coutumier ou d'une convention »²⁴⁷. Par conséquent, un acte procédural mené par les autorités judiciaires en dehors de cette hypothèse constituerait une violation de principes de droit international. Selon l'article 46bis du C.i.cr., tel que modifié par le législateur à la suite de l'arrêt Yahoo, les prestataires de services peuvent donc se voir imposer l'obligation de coopérer aux enquêtes pénales belges dès qu'ils exercent leurs activités sur le territoire national²⁴⁸.

Enfin, une dernière critique porte sur le fait que la Belgique décide souverainement, ce qui peut compromettre l'harmonisation européenne des règles relatives aux communications électroniques pour garantir la libre circulation des services²⁴⁹. Les entreprises seraient soumises à des systèmes juridiques distincts, ce qui pourrait les faire renoncer à s'adresser au marché belge afin d'échapper à cette obligation de collaboration découlant de l'article 46bis²⁵⁰.

²⁴²C.i.cr., art. 46bis, §4, al. 3.

²⁴³M. GIACOMETTI, « Chapitre 2 - La récolte transfrontière de preuves électroniques en droit belge », *op. cit.*, p. 646.

²⁴⁴M. GIACOMETTI, « Chapitre 2 - La récolte transfrontière de preuves électroniques en droit belge », *op. cit.*, p. 646.

²⁴⁵V. FRANSEN et O. LEROUX, *op. cit.*, p. 203 ; S. TOSZA, « Cross-border gathering of electronic evidence : mutual legal assistance, its shortcomings and remedies », in *Société numérique et droit pénal : Belgique, France, Europe*, Bruxelles, Bruylant, 2019, p. 276.

²⁴⁶V. FRANSEN et O. LEROUX, *op. cit.*, p. 203.

²⁴⁷C.P.I.J., 7 septembre 1927, *SS Lotus (France/Turquie)*, C.P.J.I. Rec., 1927, Série A, n° 10, pp. 18-19.

²⁴⁸M. 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 : Belgique, France, Europe*, Bruxelles, Bruylant, 2019, p. 322.

²⁴⁹A. GOSSE, « 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. 191.

²⁵⁰A. GOSSE, *op. cit.*, p. 203.

Chapitre 4 : Injonction dans le cadre d'une illégalité en matière de droits de la propriété intellectuelle (Directive 2001/29/CE et Directive 2004/48/CE)

Il existe une autre technique qui intervient uniquement dans le cadre d'une atteinte à un droit de propriété intellectuelle. Cette procédure consiste à faire intervenir les fournisseurs d'accès à internet en vue de révéler l'identité d'un auteur anonyme. Leur rôle est d'une part purement technique, consistant à donner accès à internet, et d'autre part procédural²⁵¹ dans la lutte contre le contenu illicite²⁵².

Section 1 : Base juridique

Cette procédure d'injonction repose sur une double base juridique.

Premièrement, la Directive 2001/29/CE sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information²⁵³. Cette directive prévoit que le droit d'auteur octroie le droit exclusif d'autoriser ou d'interdire toute communication au public, y compris la mise à la disposition du public de manière que chacun puisse y avoir accès de l'endroit ou au moment que l'auteur de l'œuvre choisit individuellement²⁵⁴.

Deuxièmement, la Directive 2004/48/CE sur le respect des droits de propriété intellectuelle²⁵⁵ vise à renforcer les mesures de protection des droits intellectuels. Elle établit entre autres des voies de recours efficaces permettant aux titulaires de faire respecter leurs droits. L'article 8 de cette directive prévoit un droit d'information, pour les ayants droit, sur l'origine des atteintes constatées et sur l'identité des personnes impliquées²⁵⁶. Cette disposition a été transposée à l'article XI.334, §3 du Code de droit économique.

²⁵¹P. MONVILLE et M. GIACOMETTI, « Les fournisseurs d'accès à internet, nouveaux gendarmes de la toile ? », *R.D.T.I.*, 2014/2, n° 55, p. 68.

²⁵²C. COLIN, « P2P et fournisseurs d'accès à Internet - L'implication des fournisseurs d'accès à Internet dans un modèle d'autorisation des échanges d'œuvres sur les réseaux peer-to-peer », *R.D.T.I.*, 2011/4, n° 45, p. 19.

²⁵³Directive 2001/29/CE du Parlement européen et du Conseil du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information, *J.O.C.E.*, n° L 167 du 22.06.2001.

²⁵⁴Directive 2001/29/CE du Parlement européen et du Conseil du 22 mai 2001 précitée, art. 8.

²⁵⁵Directive 2004/48/CE du Parlement européen et du Conseil du 29 avril 2004 relative aux mesures et procédures visant à assurer le respect des droits de propriété intellectuelle, *J.O.U.E.*, n° L 157 du 30 avril 2004.

²⁵⁶Directive 2004/48/CE du Parlement européen et du Conseil du 29 avril 2004 précitée, art. 8.

Section 2 : Champ d'application

L'article 8 de la Directive 2004/48/CE invite les États à prévoir des dispositions permettant aux autorités d'enjoindre à un fournisseur d'accès à internet de communiquer au titulaire d'un droit d'auteur l'identité de l'abonné correspondant à l'adresse IP à partir de laquelle une illégalité a été commise²⁵⁷. Après transposition, l'article XI.334, §3 du Code de droit économique dispose : « Lorsque dans le cadre d'une procédure, le juge constate une atteinte, il peut ordonner, à la demande de la partie habilitée à agir en contrefaçon, à l'auteur de l'atteinte de fournir à la partie qui introduit cette action toutes les informations dont il dispose concernant l'origine et les réseaux de distribution des biens ou services contrefaisants et de lui communiquer toutes les données s'y rapportant, pour autant qu'il s'agisse d'une mesure justifiée et proportionnée. »²⁵⁸

Généralement, cette demande porte sur l'identité du ou des clients ou utilisateurs des services de l'intermédiaire²⁵⁹. Les services d'intermédiaires qui peuvent être visés sont les fournisseurs d'accès à internet, les hébergeurs, les opérateurs de plateformes de partage ou de vente en ligne et les opérateurs de plateformes de réseaux sociaux.

La Cour de justice de l'Union européenne a indiqué par ailleurs que l'article 8 de la directive permettait un juste équilibre entre le droit d'information des titulaires de droit d'auteur et le droit à la protection des données à caractère personnel²⁶⁰.

Section 3 : Jurisprudence de la Cour de justice de l'Union européenne

La jurisprudence de la Cour de justice de l'Union européenne a eu une certaine influence sur cette procédure d'injonction. En effet, saisie de questions préjudicielles de la part d'autorités nationales, la Cour a eu l'occasion d'interpréter et de clarifier certains aspects de ce mécanisme.

²⁵⁷C.J.U.E., arrêt *Bonnier Audio AB e.a. c. Perfect Communication Sweden AB*, 19 avril 2012, C-461/10, §61.

²⁵⁸Code de droit économique, art. XI.334, §3.

²⁵⁹P. CAMPOLINI, S. HERMOYE, F. LEJEUNE, « Droit d'auteur et contrefaçon dans l'environnement internet : les injonctions contre les intermédiaires », *A&M*, 2017/3, p. 241.

²⁶⁰C.J.U.E. arrêt *Mircom c. Telenet BVBA*, 17 juin 2021, C-597/19, §121.

Sous-section 1 : Arrêt productores de música de España (Promusicae) c. Telefónica de España SAU

Cette obligation d'injonction a fait l'objet d'une question préjudicielle devant la grande Chambre de la Cour de justice de l'Union européenne dans l'arrêt productores de música de España c. Telefónica de España SAU, dit arrêt « Promusicae » du 29 janvier 2008²⁶¹.

Concernant les faits, Promusicae, une ASBL regroupant des producteurs et des éditeurs d'enregistrements musicaux et audiovisuels, avait demandé au Tribunal de commerce de Madrid d'ordonner à la société Telefónica, fournisseur d'accès à internet, de révéler l'identité et l'adresse physique de certains de ses utilisateurs afin de les poursuivre en justice pour atteintes à la propriété intellectuelle. Ces personnes étaient soupçonnées d'utiliser un programme *peer to peer*, « Kazaa », donnant accès à des phonogrammes dont les droits patrimoniaux d'exploitation appartiennent aux associés de Promusicae²⁶².

En première instance, Telefonica s'est vu ordonner de répondre à cette demande mais elle s'y est opposée en défendant l'argument selon lequel la loi espagnole ne l'autorisait pas à le faire dans le cadre d'une procédure civile.

La juridiction espagnole a saisi la Cour de justice de l'Union européenne dans le cadre d'une question préjudicielle. La question était de savoir si le droit européen imposait aux États membres de prévoir l'obligation de communiquer des données à caractère personnel dans le cadre d'une procédure civile visant à assurer la protection effective du droit d'auteur.

Dans son raisonnement, la Cour décide qu'il ne découle ni de cette directive ni des Directives 2000/31, 2001/29 ou 2004/48 que les États membres seraient obligés de prévoir une telle possibilité²⁶³. Toutefois, les États membres disposent d'une certaine marge de manœuvre concernant la transposition dans leur droit national des directives précitées²⁶⁴. Les États

²⁶¹C.J.U.E., arrêt Productores de Musica de Espana (Promusicae) c. Telefonica de Espana SAU, 29 janvier 2008, C-275-06.

²⁶²E. RICBOURG-ATTAL, « Section II. - Les acteurs diffuseurs du contenu de l'internet », in *La responsabilité civile des acteurs de l'internet*, 1^{re} édition, Bruxelles, Larcier, 2014, p. 174.

²⁶³C.J.U.E., arrêt Productores de Musica de Espana (Promusicae) c. Telefonica de Espana SAU, 29 janvier 2008, C-275-06, §§ 55 et 58-60.

²⁶⁴C.J.U.E., arrêt Productores de Musica de Espana (Promusicae) c. Telefonica de Espana SAU, 29 janvier 2008, C-275-06, § 67.

membres doivent, selon la Cour, faire usage de cette marge d'appréciation pour tenter d'assurer un juste équilibre entre les différents droits fondamentaux en présence²⁶⁵. D'une part, il y a le droit de propriété (intellectuelle) et le droit à une protection juridictionnelle effective de Promusicae, garantis à l'article 47 de la Charte des droits fondamentaux de l'Union européenne²⁶⁶ et à l'article 13 de la Convention européenne des droits de l'homme²⁶⁷. D'autre part, il y a le droit fondamental à la protection de la vie privée des clients de Telefonica²⁶⁸. L'enseignement de cet arrêt réside donc essentiellement dans le juste équilibre à trouver entre les intérêts en jeu²⁶⁹.

La Cour, par son arrêt du 29 janvier 2008, renvoie l'affaire au juge national pour que ce dernier décide de l'équilibre à définir.

Sous-section 2 : Ordonnance Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH c. Tele2 Telecommunication GmbH

Dans l'ordonnance Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH c. Tele2 Telecommunication GmbH, dit « LSG », rendu le 19 février 2009²⁷⁰, la Cour de justice est saisie d'une question préjudicielle de la part des autorités autrichiennes. La question était de savoir si le droit à l'information, consacré par une législation nationale transposant l'article 8 de la Directive 2004/48/CE, était conforme au droit de l'Union en matière de protection des données à caractère personnel.

La Cour répondit que la Directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques²⁷¹ n'excluait pas la possibilité pour les États membres de prévoir l'obligation de divulguer des

²⁶⁵C.J.U.E., arrêt Productores de Musica de Espana (Promusicae) c. Telefonica de Espana SAU, 29 janvier 2008, C-275-06, §§ 66-68.

²⁶⁶Charte des droits fondamentaux de l'Union européenne du 7 décembre 2000, *J.O.C.E.*, 18 décembre 2000, art. 47.

²⁶⁷Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales précitée, art. 13.

²⁶⁸C.J.U.E., arrêt Productores de Musica de Espana (Promusicae) c. Telefonica de Espana SAU, 29 janvier 2008, C-275-06, §§ 62-63.

²⁶⁹P. CAMPOLINI, S. HERMOYE et F. LEJEUNE, *op.cit.*, p. 244.

²⁷⁰C.J.U.E., ordonnance Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH c. Tele2 Telecommunication GmbH, 19 février 2009, C-557/07.

²⁷¹Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (« directive vie privée et communications électroniques »), *J.O.U.E.*, 31 juillet 2002.

données à caractère personnel dans le cadre d'une procédure civile. Toutefois, les États membres n'ont pas l'obligation de prévoir une telle procédure²⁷².

Sous-section 3 : Arrêt Bonnier audio AB e.a. c. Perfect Communication Sweden AB

Le 19 avril 2012, la Cour de justice s'est à nouveau prononcée sur l'obligation de communication de données à caractère personnel d'un abonné par un FAI dans l'arrêt Bonnier audio AB e.a. c. Perfect Communication Sweden AB²⁷³.

Une nouvelle question préjudicielle lui avait été soumise de la part des autorités suédoises. Les autorités nationales voulaient savoir si le droit de l'Union s'opposait ou non à une injonction fondée sur une disposition de droit national transposant l'article 8 de la Directive 2004/48/CE.

La Cour procéda dès lors à un examen de la disposition nationale en cause, en vue de déterminer si celle-ci assurait un juste équilibre entre les différents droits fondamentaux applicables, conformément à son arrêt Promusicae et à l'ordonnance LSG précités. Selon la Cour, la disposition permet bien d'assurer un juste équilibre²⁷⁴ car elle répond aux exigences de l'article 8 de la directive. En effet, pour qu'une injonction de communiquer les données en cause puisse être ordonnée, il faut qu'il existe tout d'abord des indices réels d'atteinte à un droit de propriété intellectuelle, ensuite les informations demandées doivent être susceptibles de faciliter l'enquête sur l'atteinte en question, et enfin les raisons motivant cette injonction doivent être d'un intérêt supérieur aux inconvénients ou autres préjudices qu'elle peut entraîner pour son destinataire ou à tout autre intérêt qui s'y oppose²⁷⁵.

Sous-section 4 : Arrêt Coty Germany GmbH c. Stadtparkasse Magdeburg

En 2015, la Cour de justice a été saisie d'une question préjudicielle de la part des autorités allemandes. L'affaire opposait une société allemande fabriquant et distribuant des parfums, Coty Germany GmbH (ci-après « Coty Germany »), à un établissement bancaire, Stadtparkasse Magdeburg (ci-après « Sparkasse »). Cette demande a été présentée dans le

²⁷²C.J.U.E., ordonnance Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH c. Tele2 Telecommunication GmbH, 19 février 2009, C-557/07.

²⁷³C.J.U.E., arrêt Bonnier Audio AB e.a. c. Perfect Communication Sweden AB., 19 avril 2012.

²⁷⁴C.J.U.E., arrêt Bonnier Audio AB e.a. c. Perfect Communication Sweden AB., 19 avril 2012, §§ 59-60.

²⁷⁵C.J.U.E., arrêt Bonnier Audio AB e.a. c. Perfect Communication Sweden AB., 19 avril 2012, §58.

cadre d'un litige au sujet du refus de cette dernière de fournir à Coty Germany des informations relatives à un compte bancaire.

Dans les faits²⁷⁶, Coty Germany a acheté en 2011, par l'intermédiaire d'une plateforme de ventes aux enchères en ligne, une bouteille de parfum de la marque « Davidoff Hot water » dont elle est détentrice. Pour conclure la vente, il fallait qu'elle verse l'argent du produit sur le compte bancaire de Sparkasse. À la réception du parfum, Coty Germany s'aperçoit que le produit est une contrefaçon ; elle demande donc à la plateforme de ventes aux enchères de lui fournir le nom réel du titulaire du compte à partir duquel le parfum a été vendu. Cette personne a reconnu être titulaire du compte, toutefois elle a nié être le vendeur de la bouteille de parfum et a refusé de fournir plus d'informations, invoquant son droit au silence.

L'entreprise Coty Germany s'est alors retournée vers l'établissement bancaire Sparkasse, afin d'obtenir les données identifiantes, à savoir le nom et l'adresse du titulaire du compte utilisé pour l'achat. Le Tribunal de première instance rend son jugement dans lequel il oblige la Sparkasse à communiquer les informations demandées. L'établissement bancaire fait appel de cette décision devant l'Oberlandesgericht Naumburg qui donne raison à Sparkasse. Coty Germany introduit par la suite un pourvoi en cassation devant le Bundesgerichtshof.

La juridiction décide alors de poser une question préjudicielle à la Cour de justice de l'Union européenne. La Cour devait déterminer si la législation nationale, autorisant un établissement bancaire à invoquer le secret bancaire pour refuser la divulgation d'informations, était conforme avec l'article 8 de la Directive 2004/48/CE.

Dans son raisonnement, la Cour a souligné qu'il y avait dans cette affaire une confrontation entre plusieurs droits fondamentaux, d'une part le droit à un recours effectif et le droit de propriété intellectuelle, et d'autre part le droit à la protection des données à caractère personnel²⁷⁷. Rappelant sa jurisprudence antérieure et la nécessité d'assurer un juste équilibre entre ces différents droits fondamentaux²⁷⁸, la Cour conclut que la disposition nationale permettant un recours illimité et inconditionnel au secret bancaire par l'établissement bancaire constituait une atteinte caractérisée au droit fondamental à un recours effectif et au droit de

²⁷⁶C.J.U.E., arrêt Coty Germany GmbH c. Stadtparkasse Magdeburg, 16 juillet 2015, C-580/13, §§9-12.

²⁷⁷C.J.U.E., arrêt Coty Germany GmbH c. Stadtparkasse Magdeburg, 16 juillet 2015, C-580/13, § 39.

²⁷⁸C.J.U.E., arrêt Coty Germany GmbH c. Stadtparkasse Magdeburg, 16 juillet 2015, C-580/13, §43.

propriété intellectuelle. Dès lors, une telle disposition ne permet pas de garantir un juste équilibre entre les différents droits fondamentaux en présence²⁷⁹.

Section 4 : Point de vue critique

L'avantage de cette procédure d'injonction est qu'elle implique les fournisseurs d'accès à internet. Ces professionnels sont les mieux placés pour faire cesser les atteintes qui ont lieu sur internet²⁸⁰, puisqu'ils peuvent lever l'anonymat d'un individu via l'adresse IP²⁸¹. Il s'agit d'une des données les plus identifiantes de l'utilisateur, permettant au fournisseur d'accès de savoir qui se cache derrière cette adresse²⁸².

L'adresse IP, de par son importance dans les procédures d'identification des individus, soulève des questions juridiques, notamment quant à sa nature. Dans un avis du 20 juin 2007 relatif au concept de données à caractère personnel, le Groupe de l'Article 29 a considéré « les adresses IP comme des données concernant une personne identifiable. [...] Les fournisseurs d'accès Internet et les gestionnaires des réseaux locaux peuvent, en utilisant des moyens raisonnables, identifier les utilisateurs Internet auxquels ils ont attribué des adresses IP, du fait qu'ils enregistrent systématiquement dans un fichier les date, heure, durée et adresse dynamique IP données à l'utilisateur Internet. Il en va de même pour les fournisseurs de services Internet qui conservent un fichier-registre sur le serveur http »²⁸³. Cette position est soutenue par plusieurs autorités nationales, telles que la Commission belge pour la vie privée de 2001²⁸⁴ et l'Agence espagnole de protection des données²⁸⁵. Toutefois, d'autres autorités nationales ne partagent pas cet avis. C'est le cas de la Cour d'appel de Paris²⁸⁶ qui, dans un de ses arrêts, a indiqué que l'adresse IP d'un appareil électronique ne permettait pas d'identifier son utilisateur. La Cour a estimé que l'obtention de l'identité de l'utilisateur nécessitait une plainte et des actes d'enquête auprès des FAI menés par les autorités judiciaires.

²⁷⁹C.J.U.E., arrêt Coty Germany GmbH c. Stadtparkasse Magdeburg, 16 juillet 2015, C-580/13, §45.

²⁸⁰F. GEORGE et J. HUBIN, *op. cit.*, p. 214.

²⁸¹E. RICBOURG-ATTAL, *op. cit.*, p. 174.

²⁸²M. UNTERSINGER, *op. cit.*, p. 72.

²⁸³Avis 4/2007 du Groupe de l'Article 29 sur le concept de données à caractère personnel, le 20 juin 2007, disponible sur https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf.

²⁸⁴Avis 5/2006 du Groupe de l'article 29 sur l'interprétation de la notion de données personnelles, 1er avril 2006, disponible sur https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp122_en.pdf.

²⁸⁵Rapport juridique 327/2003 de l'Agence espagnole de protection des données (« Carácter de dato personal de la dirección IP »), disponible sur <https://www.aepd.es/es/documento/2003-0327.pdf>.

²⁸⁶C.A. Paris, 13e ch., sect. B, 27 avril 2007, Guillemot et C.A. Paris, 13e ch., sect. A, 15 mai 2007, Sebaux.

Par ailleurs, il s'agit ici de légiférer dans un domaine fragile. Selon M. KNOCKAERT relève à ce propos « l'infernal trio que forment le droit fondamental à la propriété, la protection des données à caractère personnel et la confidentialité des communications électroniques »²⁸⁷. Il n'est donc pas étonnant que ce droit d'information pose quelques difficultés pratiques en raison des nombreux intérêts en jeu.

Enfin, cette procédure ne serait pas d'application dans le cas où le contenu a été mis en ligne à partir de cybercafés ou plus généralement de lieux publics. L'adresse IP conduira dans ce cas à l'ordinateur du cybercafé, mais il sera difficile de déterminer quel était l'individu derrière le contenu posté.

²⁸⁷M. KNOCKAERT, « Note sous C.J.U.E. (5e ch.), 17 juin 2021, C-597/19 », *R.D.T.I.*, 2021/3, n° 84, p. 85.

Partie 3 : Procédures d'obtention des preuves numériques

Après avoir dressé un état des lieux des procédures permettant de révéler l'identité des auteurs d'infractions, cette troisième partie se concentre sur les procédures d'obtention de preuves numériques.

Dans cet environnement numérique, une multitude de services de communication disponibles en ligne, d'applications, de sites web et de plateformes digitales enregistrent des informations concernant leurs utilisateurs, telles que leur identité, leurs contacts et leurs activités virtuelles. Ces informations peuvent intéresser les enquêtes pénales²⁸⁸.

Afin d'obtenir les données numériques, le droit de la procédure pénale autorise les autorités à demander l'accès à ces données aux fournisseurs de services. Toutefois, lorsque le prestataire est situé à l'étranger ou que les données se trouvent localisées en dehors du territoire national, les autorités devront passer par des procédures transfrontalières d'obtention des preuves numériques²⁸⁹. Partant de ce constat, nous allons tenter d'analyser ces différentes procédures.

Le premier chapitre se penchera sur l'analyse de la procédure de collecte transfrontalière de preuves numériques établie par la Directive 2014/41/UE. Le deuxième chapitre examinera la procédure européenne d'injonctions de production et de conservation des preuves électroniques en matière pénale, instaurée par le Règlement 2023/1543 et la Directive 2023/1544. Le dernier chapitre étudiera la procédure d'entraide judiciaire internationale utilisée dans la collecte de preuves numériques, mise en place par la Convention sur la cybercriminalité.

²⁸⁸M. GIACOMETTI, « Collecte transfrontalière de preuves numériques selon le point de vue belge. La décision d'enquête européenne, un moyen approprié ? », *op. cit.*, p. 287.

²⁸⁹S. TOSZA, *op. cit.*, p. 269.

Chapitre 1 : Collecte transfrontalière de preuves numériques (Directive 2014/41/UE)

Cette procédure de collecte transfrontalière de preuves numériques est une conséquence directe de l'utilisation croissante des technologies de l'information. D'après M. GIACOMETTI, il s'agirait d'un des instruments les plus utilisés par les États membres de l'Union européenne lorsqu'ils cherchent à récolter des preuves numériques situées en dehors de leurs frontières²⁹⁰.

La collecte de preuves numériques est une procédure qui permet de rassembler des preuves telles que l'origine du contenu illégal, l'identité de l'auteur, etc. Étant donné que ces preuves se trouvent chez l'opérateur du service²⁹¹, des règles ont dû être mises en place au niveau européen afin de permettre aux autorités de les collecter.

Il convient de souligner le fait que ces règles de collecte de preuves numériques doivent intervenir dans le respect des libertés fondamentales, telles que le droit à la vie privée ou les règles en matière de protection de données personnelles²⁹².

Section 1 : Base juridique

Cette procédure de collecte transfrontalière de preuves numériques trouve sa base juridique dans la Directive européenne 2014/41/UE concernant la décision d'enquête européenne en matière pénale²⁹³. L'adoption de cette Directive est intervenue suite à une proposition formulée par sept États membres : Belgique, Bulgarie, Estonie, Espagne, Autriche, Slovaquie et Suède. Elle a été transposée en droit belge par une loi du 22 mai 2017²⁹⁴.

²⁹⁰M. GIACOMETTI, « Conclusion de la Partie II - La récolte transfrontière de preuves électroniques au moyen des instruments d'entraide judiciaire : un premier pilier du modèle de récolte de preuves électroniques (accessibles localement) », in *La récolte transfrontière de preuves électroniques dans le contexte européen*, 1^{re} édition, Bruxelles, Bruylant, 2023, p. 445.

²⁹¹B. DOCQUIR, *op. cit.*, p. 601.

²⁹²*Ibid.*

²⁹³Directive 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.

²⁹⁴Loi du 22 mai 2017 relative à la décision d'enquête européenne en matière pénale, *M.B.*, 23 avril 2017.

Section 2 : Champ d'application

En vertu de l'article premier de la directive, il s'agit d'une décision judiciaire qui a été émise ou validée par une autorité judiciaire d'un État membre (État d'émission) afin de faire exécuter une ou plusieurs mesures d'enquête spécifique sur le territoire d'un autre État membre (État d'exécution) en vue d'obtenir des preuves qui s'y trouvent localisées ou qui se trouvent déjà en possession de l'Etat membre d'exécution²⁹⁵.

Cette procédure est basée sur le principe de reconnaissance mutuelle entre États membres, qui a pour effet que chaque État de l'Union doit reconnaître et donner suite à cette demande. Par ailleurs, une telle procédure peut être utilisée aux fins de recueillir tout type de preuve²⁹⁶, y compris des preuves numériques²⁹⁷. M. GIACOMETTI indique que les preuves électroniques sont « des informations qui se trouvent sous forme électronique et qui sont traitées, stockées ou transmises via un système informatique et qui disposent d'une valeur probante potentielle »²⁹⁸.

Pour que la décision judiciaire émise soit valide, il convient de respecter certaines conditions²⁹⁹. Premièrement, l'autorité judiciaire doit être compétente, c'est-à-dire qu'un juge, un juge d'instruction ou un procureur doit être compétent dans le cadre de la procédure en cours³⁰⁰. Deuxièmement, il convient de respecter le droit national de l'Etat d'émission³⁰¹. Troisièmement, la décision d'enquête doit respecter les conditions de proportionnalité et de nécessité³⁰².

Selon l'article 4 de la directive, la décision peut être émise à des fins d'enquête « à engager » par l'autorité judiciaire³⁰³. Il n'est donc pas nécessaire que la procédure pénale ait déjà été

²⁹⁵Directive 2014/41/UE du Parlement européen et du Conseil du 3 avril 2014 précitée, art. 1, §1.

²⁹⁶Directive 2014/41/UE du Parlement européen et du Conseil du 3 avril 2014 précitée, considérant 8.

²⁹⁷M. GIACOMETTI, « Collecte transfrontalière de preuves numériques selon le point de vue belge. La décision d'enquête européenne, un moyen approprié ? », *op. cit.*, p. 288.

²⁹⁸M. GIACOMETTI, « La récolte transfrontière de preuves électroniques dans le contexte européen. Construction d'un modèle à l'aune d'une nouvelle conception de la souveraineté des États », *A.D.L.*, 2019/3, p. 423.

²⁹⁹M. GIACOMETTI, « Chapitre 1er - La récolte de preuves électroniques au moyen de la décision d'enquête européenne : un instrument adapté ? », in *La récolte transfrontière de preuves électroniques dans le contexte européen*, 1^{re} édition, Bruxelles, Bruylant, 2023, pp. 279.

³⁰⁰Directive 2014/41/UE du Parlement européen et du Conseil du 3 avril 2014 précitée, art. 2, c), i.

³⁰¹Directive 2014/41/UE du Parlement européen et du Conseil du 3 avril 2014 précitée, art. 6, §1, b).

³⁰²Directive 2014/41/UE du Parlement européen et du Conseil du 3 avril 2014 précitée, art. 6, §1, a).

³⁰³Directive 2014/41/UE du Parlement européen et du Conseil du 3 avril 2014 précitée, art. 4, a).

engagée par l'autorité de l'Etat d'émission. Dès lors, il est possible d'agir proactivement afin de recueillir des preuves concernant l'identité d'un individu sur les réseaux sociaux³⁰⁴.

Section 3 : Point de vue critique

Une première critique que l'on peut émettre est que la notion de preuve numérique ne fait pas l'objet d'une définition en droit européen. On retrouve, par contre, une définition en droit belge dans les travaux préparatoires de la loi du 28 novembre 2000 sur la criminalité informatique³⁰⁵ : « Les données informatiques constituent les représentations de l'information pouvant être stockées, traitées et transmises par le biais d'un système informatique. »³⁰⁶ Cette définition correspond à l'article 1, b) de la Convention sur la cybercriminalité du 23 décembre 2001 : « Toute représentation de fait, d'informations ou de concepts sous une forme qui se prête à un traitement informatique y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction. »³⁰⁷

Ensuite, de manière plus positive, M. GIACOMETTI estime que cette décision d'enquête européenne se révèle être une révolution pour la coopération judiciaire en matière pénale entre les États membres, parce qu'il s'agit de récolter des preuves en dehors de leurs frontières, sur la base d'une procédure stricte fondée sur le principe de reconnaissance mutuelle, au moyen d'un simple formulaire uniformisé à remplir.³⁰⁸

Enfin, d'une manière générale, plusieurs auteurs estiment que cette procédure n'est pas adaptée aux technologies et aux besoins actuels³⁰⁹ et qu'elle aurait dès lors besoin d'une révision pour gagner en efficacité.

³⁰⁴M. GIACOMETTI, « Chapitre 1er - La récolte de preuves électroniques au moyen de la décision d'enquête européenne : un instrument adapté ? », *op. cit.*, p. 271.

³⁰⁵Loi du 28 novembre 2000 sur la criminalité informatique, *M.B.*, 3 février 2001.

³⁰⁶Projet de loi relatif à la criminalité informatique, *Doc. parl.*, ch. repr., sess. ord., 1999-2000, n°50-213/001, p.12.

³⁰⁷Convention du 23 novembre 2001 du Conseil de l'Europe sur la cybercriminalité, signée à Budapest le 23 novembre 2001, art. 1, b).

³⁰⁸M. GIACOMETTI, « Collecte transfrontalière de preuves numériques selon le point de vue belge. La décision d'enquête européenne, un moyen approprié ? », *op. cit.*, p. 323.

³⁰⁹M. GIACOMETTI, « Chapitre 2 - La récolte de preuves électroniques grâce aux dispositions spécifiques d'entraide contenues dans la Convention de Budapest : une plus-value ? », *op. cit.*, p. 365. ; S. TOSZA, *op. cit.*, p. 270.

Chapitre 2 : Injonctions européennes de production et de conservation des preuves électroniques en matière pénale (Règlement 2023/1543 et Directive 2023/1544)

Les lacunes du cadre juridique de la collecte transfrontalière de preuves numériques et la nécessité de s'adapter aux besoins actuels ont été entendues par le législateur européen³¹⁰, qui a mis en place une procédure d'injonctions européennes de production et de conservation des preuves électroniques en matière pénale. Cette procédure ne vise pas à remplacer la Directive 2014/41/UE concernant la décision d'enquête européenne en matière pénale, mais elle fournit un outil supplémentaire aux autorités³¹¹.

Section 1 : Règlement (UE) 2023/1543 du 12 juillet 2023 relatif aux injonctions européennes de production et de conservation concernant les preuves électroniques dans le cadre des procédures pénales et aux fins de l'exécution de peines privatives de liberté prononcées à l'issue d'une procédure pénale

En 2018, la Commission européenne a présenté une proposition de Règlement concernant les injonctions européennes de production et de conservation de preuves électroniques en matière pénale³¹². Dans cette proposition, la Commission exprimait des préoccupations quant aux initiatives nationales visant à garantir un accès rapide aux preuves numériques³¹³. Elle souhaitait faire face aux défis du numérique et fournir des outils judiciaires et répressifs adaptés aux modes de communication des criminels et aux nouvelles formes de criminalité³¹⁴.

Pour ce faire, voulant assurer une coopération efficace entre États membres en matière de collecte de preuves numériques, la Commission proposa d'instaurer une procédure d'injonctions européennes de production et de conservation dans le but de simplifier l'obtention

³¹⁰S. TOSZA, *op. cit.*, p. 277.

³¹¹Proposition 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, §61.

³¹²Proposition 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.

³¹³ 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.

³¹⁴ 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,

et la collecte, dans le cadre de procédures pénales, des preuves électroniques stockées ou détenues par des fournisseurs de services relevant d'une autre juridiction³¹⁵.

Le Règlement du 12 juillet 2023 relatif aux injonctions européennes de production et de conservation concernant les preuves électroniques dans le cadre des procédures pénales et aux fins de l'exécution de peines privatives de liberté prononcées à l'issue d'une procédure pénale a donc été adopté³¹⁶.

L'article premier de ce règlement permet à une autorité de contraindre un fournisseur de services offrant des prestations au sein de l'Union européenne et établi dans un autre Etat membre (ou s'il n'est pas établi, représenté par un représentant légal dans un autre Etat membre) de produire ou de conserver des preuves électroniques, indépendamment de l'emplacement des données.

L'élément essentiel de ce règlement est que l'ordre de production ou de conservation de preuves passe directement de l'autorité émettrice d'un Etat membre au prestataire de services. Dès lors, il n'y a, en principe, pas d'intervention d'une autorité de l'Etat d'exécution³¹⁷.

Le règlement prévoit trois catégories d'autorités qui pourront intervenir dans le cadre de cette procédure³¹⁸. Premièrement, il y a les autorités habilitées à délivrer les deux demandes, à savoir la production et la conservation de tout type de données. Il s'agit des juges, tribunaux, juges d'instruction. Deuxièmement, il y a les procureurs, dont la compétence est limitée aux mesures moins sensibles³¹⁹. Troisièmement, nous retrouvons « toute autre autorité compétente définie par l'Etat d'émission qui, dans le cas d'espèce, agit en qualité d'autorité d'enquête dans le cadre d'une procédure pénale et qui est compétente pour ordonner la collecte de preuves conformément au droit national »³²⁰.

³¹⁵Proposition 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.

³¹⁶Règlement (UE) 2023/1543 du Parlement européen et du Conseil du 12 juillet 2023 relatif aux injonctions européennes de production et aux injonctions européennes de conservation concernant les preuves électroniques dans le cadre des procédures pénales et aux fins de l'exécution de peines privatives de liberté prononcées à l'issue d'une procédure pénale, J.O.U.E, 28 juillet 2023.

³¹⁷S. TOSZA, *op. cit.*, p. 278.

³¹⁸S. TOSZA, *op. cit.*, p. 280.

³¹⁹Règlement (UE) 2023/1543 du Parlement européen et du Conseil du 12 juillet 2023 précité, considérant 30.

³²⁰S. TOSZA, *op. cit.*, p. 280.

Par ailleurs, cette injonction devra être transmise au destinataire au moyen d'un certificat d'accompagnement de l'injonction européenne de production (EPOC) ou au certificat d'accompagnement de l'injonction européenne de conservation (EPOC-PR), comme prévu à l'article 9 du Règlement³²¹.

Enfin, afin de rendre la procédure plus efficace, le règlement impose des délais d'exécution assez courts³²². Concernant la procédure de production de données, l'article 10, §3 et 4 du règlement prévoit un délai de 10 jours en temps normal et 8h en cas d'urgence³²³. Concernant la procédure de conservation de données, l'article 11, §1 indique que la demande doit être exécutée « sans retard justifié »³²⁴.

Ce règlement, tout juste adopté par le Parlement et le Conseil le 12 juillet 2023, sera d'application à partir du 18 août 2026³²⁵.

Section 2 : Directive (UE) 2023/1544 du 12 juillet 2023 établissant des règles harmonisées concernant la désignation d'établissements désignés et de représentants légaux aux fins de l'obtention de preuves électroniques dans le cadre des procédures pénales

Afin de rendre efficace la procédure, prévue par le Règlement 2023/1543, cette directive oblige l'État membre à prévoir un cadre garantissant l'existence d'un représentant légal connu et habilité à qui la demande peut être adressée³²⁶.

Ainsi, l'article premier indique que la directive prévoit « des règles relatives à la désignation d'établissements désignés et de représentants légaux de certains fournisseurs de services qui proposent des services dans l'Union pour la réception, le respect et l'exécution des décisions et des injonctions émises par les autorités compétentes des États membres aux fins de l'obtention de preuves dans le cadre de procédures pénales »³²⁷.

³²¹Règlement (UE) 2023/1543 du Parlement européen et du Conseil du 12 juillet 2023 précité, considérant 55.

³²²S. TOSZA, *op. cit.*, p. 281.

³²³Règlement (UE) 2023/1543 du Parlement européen et du Conseil du 12 juillet 2023 précité, art. 10, §§3- 4.

³²⁴Règlement (UE) 2023/1543 du Parlement européen et du Conseil du 12 juillet 2023 précité, art. 11, §1.

³²⁵Règlement (UE) 2023/1543 du Parlement européen et du Conseil du 12 juillet 2023 précité, art. 34, §2.

³²⁶S. TOSZA, *op. cit.*, p. 278.

³²⁷Directive (UE) 2023/1544 du Parlement européen et du Conseil du 12 juillet 2023 établissant des règles harmonisées concernant la désignation d'établissements désignés et de représentants légaux aux fins de l'obtention de preuves électroniques dans le cadre des procédures pénales, *J.O.U.E.*, 28 juillet 2023, art. 1.

En vertu de l'article 3, §1 de la directive, les États membres doivent veiller à ce que les fournisseurs de services des services dans l'Union désignent au moins un destinataire pour la réception, le respect et l'exécution des décisions et des injonctions. Ce destinataire peut être, selon les cas, soit un établissement, soit un représentant légal³²⁸.

Les États membres ont jusqu'au 18 février 2026 au plus tard pour transposer le texte³²⁹.

Chapitre 3 : Entraide judiciaire internationale dans la collecte de preuves numériques (Convention sur la cybercriminalité du Conseil de l'Europe)

Section 1 : Base juridique

La procédure d'entraide judiciaire est prévue aux articles 23 à 34 de la Convention de Budapest sur la cybercriminalité adoptée par le Conseil de l'Europe le 23 novembre 2001³³⁰.

Cette convention a été signée et ratifiée par 63 pays dont les États-Unis, le Canada, le Japon et l'Afrique du Sud. La Belgique l'a signée le 23 novembre 2001, et l'a ratifiée par la loi du 3 août 2012³³¹.

Section 2 : Champ d'application

L'article 23 de cette convention s'articule autour de trois principes.

Premièrement, les parties ayant ratifié la convention sont tenues de coopérer dans la mesure la plus large possible ensemble, en réduisant les obstacles à la circulation rapide de l'information et des preuves³³². Ce principe est de nature à rendre la coopération plus souple par rapport au principe de réciprocité imposé dans d'autres conventions internationales³³³. Pour ce faire, la convention prévoit notamment que les parties s'informent de manière spontanée des résultats

³²⁸Directive (UE) 2023/1544 du Parlement européen et du Conseil du 12 juillet 2023 précitée, art. 3, §1.

³²⁹Directive (UE) 2023/1544 du Parlement européen et du Conseil du 12 juillet 2023 précitée, art. 7.

³³⁰Convention du 23 novembre 2001 du Conseil de l'Europe sur la cybercriminalité, signée à Budapest le 23 novembre 2001.

³³¹Loi du 3 août 2012 portant assentiment à la Convention sur la cybercriminalité faite à Budapest le 23 novembre 2001, *M.B.*, 21 novembre 2012.

³³²Convention du 23 novembre 2001 du Conseil de l'Europe sur la cybercriminalité précitée, art. 23.

³³³M. GIACOMETTI, « Chapitre 2 - La récolte de preuves électroniques grâce aux dispositions spécifiques d'entraide contenues dans la Convention de Budapest : une plus-value ? », *op. cit.*, p. 369.

d'enquêtes relatives à des infractions, lorsque ces informations peuvent être utiles à l'une ou l'autre partie³³⁴.

Deuxièmement, la convention intervient aux fins d'investigation ou de procédure concernant les infractions pénales liées à des systèmes et données informatiques, mais aussi afin de recueillir des preuves d'une infraction pénale sous forme électronique.

Troisièmement, il convient de souligner le caractère subsidiaire de la convention³³⁵, qui n'est pas un instrument qui se suffit à lui seul³³⁶ : la convention n'annule ni ne remplace pas les dispositions d'autres conventions qui trouveraient à s'appliquer³³⁷.

Cette procédure d'entraide judiciaire internationale est importante notamment dans la collecte de preuves numériques. Tout d'abord, la Convention de Budapest définit ce que sont des données informatiques comme suit : « Toute représentation de faits ou de concepts sous une forme qui se prête à un traitement informatique. »³³⁸

Ensuite, la convention distingue à cet égard trois catégories de données informatiques³³⁹. La première concerne les données relatives aux abonnés. Il s'agit d'une catégorie résiduaire³⁴⁰ dans laquelle se trouvent les données relatives autres que les données relatives au trafic et au contenu³⁴¹. Nous retrouvons ainsi les informations relatives aux types de services utilisés (téléphone mobile, messagerie téléphonique, renvoi d'appel) par l'utilisateur, l'identité de ce dernier, son adresse (postale ou électronique), son numéro de téléphone, etc.³⁴². La seconde catégorie porte sur les données relatives au trafic. Enfin, la dernière catégorie concerne les données relatives au contenu.

³³⁴Y. POULLET, « La lutte contre le racisme et la xénophobie sur internet », *op. cit.*, p. 409.

³³⁵Convention du 23 novembre 2001 du Conseil de l'Europe sur la cybercriminalité précitée, art. 39.

³³⁶M. GIACOMETTI, « Chapitre 2 - La récolte de preuves électroniques grâce aux dispositions spécifiques d'entraide contenues dans la Convention de Budapest : une plus-value ? », *op. cit.*, p. 370.

³³⁷Rapport explicatif de la convention sur la cybercriminalité du 23 novembre 2001, S.T.C.E. n°185, p. 49.

³³⁸Rapport explicatif de la convention sur la cybercriminalité du 23 novembre 2001, S.T.C.E. n°185, p. 6.

³³⁹M. GIACOMETTI, « Collecte transfrontalière de preuves numériques selon le point de vue belge. La décision d'enquête européenne, un moyen approprié ? », *op. cit.*, p. 290.

³⁴⁰M. GIACOMETTI, « Chapitre 2 - La récolte de preuves électroniques grâce aux dispositions spécifiques d'entraide contenues dans la Convention de Budapest : une plus-value ? », *op. cit.*, p. 370.

³⁴¹Convention du 23 novembre 2001 du Conseil de l'Europe sur la cybercriminalité précitée, art. 18, §3.

³⁴²M. GIACOMETTI, « Chapitre 2 - La récolte de preuves électroniques grâce aux dispositions spécifiques d'entraide contenues dans la Convention de Budapest : une plus-value ? », *op. cit.*, p. 380.

Section 3 : Point de vue critique

Cet instrument lie les États parties à la convention : les États européens mais également des États tiers, tels que les États-Unis, où se trouvent majoritairement les plateformes de réseaux sociaux³⁴³. Cette méthode est donc d'une grande importance pour les enquêtes pénales, étant donné que les principaux fournisseurs (Google (YouTube), Meta (Facebook, Instagram, WhatsApp), etc.) sont américains. L'étendue territoriale de cette convention présente donc un avantage considérable.

Un deuxième avantage est que cette convention est entièrement consacrée à la cybercriminalité³⁴⁴, les États parties voulant mener une politique pénale destinée à protéger la société de la criminalité du cyberspace.

Certains auteurs soutiennent cependant que ce dispositif n'est pas adapté aux technologies actuelles³⁴⁵. La considérant comme lourde d'un point de vue administratif, on lui reproche une certaine lenteur de procédure³⁴⁶. Par ailleurs, la convention est décrite comme ayant un caractère trop général et subsidiaire³⁴⁷, laissant trop de marge de manœuvre aux États parties. Enfin, la convention ne prévoit pas de sanctions lorsqu'un État ne respecte pas certaines obligations³⁴⁸.

La faiblesse de la convention a également été utilisée comme argument intervenu dans l'affaire Yahoo de la Cour de cassation belge. Les désavantages de cette procédures obligent en effet parfois les autorités à en contourner les règles³⁴⁹. D'après L. KERZMANN, la décision de la Cour de cassation de condamner Yahoo à collaborer avec les autorités judiciaires belges « présente

³⁴³M. GIACOMETTI, « Chapitre 2 - La récolte de preuves électroniques grâce aux dispositions spécifiques d'entraide contenues dans la Convention de Budapest : une plus-value ? », *op. cit.*, p. 366.

³⁴⁴*Ibid.*

³⁴⁵A. GOSSE, *op. cit.*, p. 197. ; M. GIACOMETTI, « Chapitre 2 - La récolte de preuves électroniques grâce aux dispositions spécifiques d'entraide contenues dans la Convention de Budapest : une plus-value ? », *op. cit.*, p. 427.

³⁴⁶*Ibid.*

³⁴⁷M. GIACOMETTI, « Chapitre 2 - La récolte de preuves électroniques grâce aux dispositions spécifiques d'entraide contenues dans la Convention de Budapest : une plus-value ? », *op. cit.*, p. 427.

³⁴⁸A. GOSSE, *op. cit.*, p. 197.

³⁴⁹S. CARRERA, G. GONZALEZ FUSTER, E. GUILD et V. MILTSILEGAS, *Acces to Electronic Data by Third-Country Law Enforcement authorities*, Center for European Policy Studies, Bruxelles, 2015.

un intérêt pratique évident, dans la mesure où la procédure d'entraide judiciaire (...) est souvent source de lenteurs et de complications administratives »³⁵⁰.

D'après les critiques émises, une réforme de la Convention est souhaitable³⁵¹.

Section 4 : Deuxième Protocole additionnel relatif au renforcement de la coopération et de la divulgation de preuves électroniques du 12 mai 2022

Ce souhait semble avoir été exaucé grâce à l'adoption en 2022 du Deuxième Protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques³⁵². Depuis le 12 mai 2022, le protocole est ouvert à la signature des États parties³⁵³.

Dans le préambule de ce deuxième protocole, il est indiqué que les technologies de l'information et de la communication sont de plus en plus utilisées et que la cybercriminalité, perçue comme une menace pour la démocratie, l'état de droit et les droits de l'homme, est en augmentation³⁵⁴. Le préambule reconnaît également l'importance de la protection des victimes de cybercriminalité³⁵⁵ et du devoir de mener des enquêtes et des poursuites criminelles efficaces pour préserver la société³⁵⁶.

L'article 7 de ce protocole concerne la divulgation directe de données relatives aux abonnés. Il prévoit que chaque partie doit adopter des mesures habilitant les autorités compétentes à adresser directement à un fournisseur de services situé sur le territoire d'une autre partie à la convention une injonction de produire des données spécifiques et stockées relatives à des abonnés. Ces données doivent être en la possession ou sous le contrôle du fournisseur, lorsqu'elles sont nécessaires à des enquêtes ou des procédures pénales spécifiques menées par la partie émettrice³⁵⁷.

³⁵⁰L. KERZMANN, « L'affaire Yahoo ! ou à qui s'adresse l'obligation de collaboration instaurée par l'article 46bis du Code d'instruction criminelle ? », *R.D.T.I.*, 2011/3, n°44, p.123.

³⁵¹A. GOSSE, *op. cit.*, p. 197.

³⁵²Deuxième Protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques, 28 février 2023, S.T.C.E n°224.

³⁵³Voy. la liste des signatures disponible sur <https://www.coe.int/fr/web/conventions/full-list?module=signatures-by-treaty&treatyenum=224> (août 2023)

³⁵⁴Deuxième Protocole additionnel à la Convention sur la cybercriminalité précité, préambule.

³⁵⁵Deuxième Protocole additionnel à la Convention sur la cybercriminalité précité, préambule.

³⁵⁶Deuxième Protocole additionnel à la Convention sur la cybercriminalité précité, préambule.

³⁵⁷Deuxième Protocole additionnel à la Convention sur la cybercriminalité précité, art. 7.

D'autres dispositions pertinentes méritent d'être mentionnées, comme l'article 8 qui vise à mettre en œuvre les injonctions d'une autre partie ordonnant la production accélérée de données relatives aux informations sur les abonnés et au trafic³⁵⁸, ainsi que l'article 10 qui traite des demandes d'entraide urgente³⁵⁹.

³⁵⁸Deuxième Protocole additionnel à la Convention sur la cybercriminalité précité, art. 8.

³⁵⁹Deuxième Protocole additionnel à la Convention sur la cybercriminalité précité, art. 10.

Conclusion

L'objectif de ce travail était de dresser un état des lieux des procédures existantes permettant de révéler l'identité d'un auteur d'infraction sur les réseaux sociaux lorsque ce dernier est anonyme.

Cette étude a d'abord mis en lumière la complexité de l'équilibre entre des droits fondamentaux, à savoir la liberté d'expression et le droit à la vie privée, dans le contexte des réseaux sociaux. À ce sujet, nous avons identifié une tendance suggérant que l'identité des auteurs d'infractions doit pouvoir être révélée pour éviter l'impunité totale. Cela nous a naturellement amené à analyser les procédures d'identification de ces individus. Enfin, l'analyse de ces procédures nous a poussé à analyser les mécanismes de collecte de preuves numériques transfrontalières, indispensables dans le contexte de répression des infractions sur les réseaux sociaux.

Au terme de ce travail, nous pouvons tirer plusieurs conclusions.

Tout d'abord, les procédures de corégulation nous semblent mieux adaptées que les règles d'autorégulation dans la recherche de l'identité des auteurs d'infractions. Nous avons constaté que les mécanismes d'autorégulation permettent éventuellement de sanctionner des comportements inadéquats, mais ne semblent pas prévoir concrètement de procédures permettant de révéler l'identité d'un individu. Les mesures de corégulation, par contre, proposent de véritables mesures concrètes, par exemple en permettant aux autorités de forcer les plateformes à collaborer pour arriver à révéler l'identité d'un individu.

Ensuite, nous identifions des lacunes concernant les droits des victimes. Les procédures actuelles sont en effet de la compétence des autorités. Le rôle de la victime est actuellement, uniquement secondaire et consiste à réunir les preuves nécessaires pour aider les enquêteurs dans leurs recherches³⁶⁰. La victime est contrainte de déposer plainte pour pouvoir obtenir l'identité de l'auteur de l'infraction dont elle est victime, et ce même si elle souhaite uniquement obtenir réparation du préjudice subi. Actuellement, la victime doit passer par la voie pénale, ce qui peut entraîner des inconvénients tels que la longueur des procédures. Il n'est en effet pas

³⁶⁰Voy. annexe, question 9 de la retranscription de l'entretien avec Monsieur OLIVIER BOGAERT, membre de la *Federal Computer Crime Unit* (FCCU), le 31 juillet 2023,

inhabituel que plusieurs années s'écoulent entre le moment du dépôt de la plainte et le résultat³⁶¹. Des incertitudes procédurales pourraient apparaître, telles que le risque de perte de données, qui parfois ne sont conservées que pendant de courtes périodes³⁶², etc. Des voix se font entendre pour réformer ce système afin d'octroyer davantage de droits à la victime. À ce sujet, nous avons évoqué la proposition de modification de l'article XII.20, §2 du Code de droit économique proposé par H. JACQUEMIN³⁶³. Toutefois, bien que cette proposition octroierait davantage de droits à la victime, cela resterait via la voie pénale et non civile. A. ADAM propose dès lors d'octroyer la compétence d'obtenir l'identité d'individu au tribunal de première instance³⁶⁴ pour que la victime puisse avoir le choix entre la voie pénale ou la voie civile.

Enfin, nous avons identifié une critique récurrente concernant l'inadaptation des mesures en vigueur face aux évolutions rapides des technologies numériques³⁶⁵. En effet, plusieurs procédures que nous avons analysées ont été adoptées à une époque où les réalités informatiques étaient bien différentes.

Malgré les limites que nous venons d'exposer, des perspectives intéressantes se dessinent pour l'avenir. Nous avons de fait identifié des évolutions législatives. Tout d'abord, le Règlement (UE) 2022/2065 (DSA), qui entrera en application en 2024, vient réformer la Directive 2000/31/CE et ajouter de nouvelles obligations de diligence à charge des plateformes. Ensuite, le Règlement 2023/1543 et la Directive 2023/1544 ajoutent une nouvelle procédure en matière de collecte de preuves numériques, à savoir un mécanisme d'injonction de production et de conservation des preuves électroniques ; ce dispositif est prévu pour 2026. Enfin, la mise en place du Deuxième Protocole additionnel à la Convention sur la cybercriminalité témoigne de l'engagement à améliorer la coopération internationale en matière de collecte de preuves numériques.

Ces futurs instruments attestent de la volonté du législateur de s'adapter aux réalités numériques actuelles pour pouvoir lutter efficacement contre la cybercriminalité.

³⁶¹A. ADAM, *op. cit.*, 95-96.

³⁶²A. ADAM, *op. cit.*, pp. 101-102.

³⁶³H. JACQUEMIN, *op.cit.*, pp. 80-81.

³⁶⁴A. ADAM, *op. cit.*, pp. 101-102.

³⁶⁵E. MONTERO, *op. cit.*, p. 388.

Annexe : Entretien avec Monsieur Olivier Bogaert, membre de la *Federal Computer Crime Unit* (FCCU), le 31 juillet 2023

Question 1 : Pouvez-vous vous présenter brièvement, quelle fonction occupez-vous et depuis combien de temps ?

« Je suis au sein de la *Computer Crime Unit*, qui gère le numérique, depuis 1998. En fait, on a créé l'équipe à la police judiciaire du parquet puis ça a été globalisé. On avait une équipe du même style à la gendarmerie et une équipe du même style à la police du Parquet et puis ça a été fusionné. On a maintenant deux structures : la FCCU à laquelle j'appartiens, c'est la CCU fédérale et les RCCU, qui sont les CCU régionales. Elles travaillent sur les dossiers que le magistrat de l'arrondissement en question peut leur procurer, en leur demandant des vérifications, des analyses. Et on a également, au niveau de la FCCU, le contact international quand les auteurs sont à distance, on travaille avec des plateformes internationales comme EUROPOL, INTERPOL pour essayer de remonter vers les auteurs. »

Question 2 : Depuis la création de la FCCU, est ce que selon vous les infractions ont évolué sur les réseaux sociaux ? Si oui, comment ?

« Oui, elles ont évolué parce que les auteurs se documentent de façon beaucoup intense que dans le passé. Ils vont par exemple chercher des informations sur les réseaux sociaux sur telle ou telle personne. Ils vont également se documenter sur les outils qui sont à disposition via les moteurs de recherche.

A ce moment-là, ils peuvent être extrêmement précis. Ils peuvent dire, par exemple : « Bon les amis, j'ai créé un nouveau profil sur Facebook. Le profil initial va être uniquement associé à mon boulot. Je vous invite à me rejoindre sur ce compte ci. » Les gens qui reçoivent ce message ne réfléchissent pas, ne prennent pas contact et vont automatiquement voir le profil, se connecter, accepter de devenir amis et donc vont mettre à disposition toutes leurs informations personnelles. Ça, ça leur permet de cibler avec précision d'autres personnes ensuite.

Moi je dis souvent aux gens, par rapport aux réglages, d'aller vérifier la sécurité et par exemple qui peut voir mon adresse mail et numéro de téléphone, « moi uniquement » ou « mes amis ».

Mais mes amis n'ont pas besoin de voir ça, parce qu'ils ont à ce moment-là contact avec moi via le profil, donc ce n'est pas ça qui les intéresse. Le problème est que le gars qui crée un profil et qui accepte des gens sans les connaître, ceux-ci pourront voir les informations personnelles comme l'adresse mail, et c'est comme ça qu'on reçoit un mail soi-disant d'une structure officielle, etc. »

Question 3 : Sur l'ensemble de vos affaires, dans quelle proportion êtes-vous amené à révéler l'identité des individus ? Est-ce que c'est une majorité ou est-ce que vous avez, au contraire, souvent accès initialement à l'identité ?

« Ça dépend un peu de la localisation. Les auteurs, arnaqueurs ou pirates vont beaucoup utiliser les outils numériques comme le VPN, qui va masquer les adresses IP d'origine. Donc il faut vérifier à l'international les tendances pour voir si d'autres États ont déjà reçu des notifications ou ont pu avancer dans les recherches. Ce n'est pas facile tout de suite de savoir où sont les informations. Mais bon, parfois ils font des petites erreurs. Par exemple, admettons qu'ils créent une adresse mail et que cette adresse mail est utilisée alors qu'ils utilisent un VPN pour d'autres activités (faux sites, etc.). Là, avec les hébergeurs avec Google, s'ils ont créé une adresse Gmail, on demande à Google via un réquisitoire du magistrat, de donner des informations.

On a des équipes, pas au niveau de la FCCU, mais des équipes des unités spéciales. Ils sont considérés comme les « *white partners* ». Mais il faut toujours le réquisitoire du magistrat pour qu'eux puissent prendre contact. Par exemple, j'ai un collègue que je connais bien, quand il a le réquisitoire, il envoie un mail à Facebook et dans les deux heures suivantes Facebook répond. »

Question 4 : Combien de temps prennent les procédures pour lever l'anonymat de quelqu'un ?

« Tout dépend de la façon dont on va accéder à certaines données. Ça peut être rapide si on a une petite erreur de l'auteur qui a laissé des informations, comme un numéro qui figurerait dans des messages adressés aux victimes par exemple. On peut à ce moment-là essayer de remonter jusqu'à lui. Mais ce n'est pas toujours évident parce qu'on se rend compte que pour certaines arnaques, par exemple l'arnaque Microsoft, c'est l'Inde ; des arnaques au sentiment basé en Afrique ; etc. C'est toujours difficile. Maintenant on a des contacts à l'international avec

certaines personnes pour pouvoir avancer dans ce domaine, mais ce n'est pas toujours très facile. »

Question 5 : Comment se passe la collaboration avec les plateformes des réseaux sociaux ? Sont-elles coopératives ? Ou au contraire réticentes ?

« Ils ont des obligations avec les règlements au niveau européen, notamment le Règlement de protection des données. Ils savent qu'ils risquent des sanctions s'ils ne sont pas coopératifs par rapport à des enquêtes judiciaires. Ils ont des équipes maintenant. Et l'avantage qu'on a aussi est que maintenant Google est en Belgique. Google a son data center à Saint Ghislain dans la région Montoise et Google est aussi installé dans le quartier Schuman dans le centre de Bruxelles. Il suffit de prendre contact avec eux en demandant des informations, mais toujours dans l'obligation de disposer d'un réquisitoire du magistrat. »

Question 6 : Selon vous, quels sont les principaux obstacles à l'identification d'un individu anonyme sur les réseaux sociaux ?

« Le problème c'est que des fausses identités sont souvent utilisées. Comme je le disais, on usurpe l'identité de quelqu'un et donc on utilise des outils techniques très pointus qui empêchent de voir quelle est l'origine de la création de ce profil. Donc tout dépend de la façon dont l'auteur va commettre une petite erreur à moment donné.

Dans un premier temps, quand on demande qui est à l'origine de la création de ce profil, tout de suite on reçoit des messages « excusez-nous mais les adresses IP sont complètement masquées » ou alors « l'adresse IP correspond à un autre pays que le pays que la personne renseigne ». Et donc on peut se retrouver avec un hébergeur ou une structure qui fournit des VPN. Les données sont cryptées, donc c'est un peu complexe. Maintenant l'hébergeur peut collaborer sur base d'un réquisitoire et il peut essayer d'analyser qui a créé à tel moment et essayer de voir s'il peut retrouver l'adresse IP d'origine. Mais souvent ils utilisent plusieurs outils. En utilisant un VPN sur leur ordinateur, l'adresse IP qui va apparaître sur le serveur dans lequel il demande un VPN également, ça sera une adresse IP complètement masquée qu'on ne peut pas identifier. »

Question 6bis : De ce que je comprends, il y a plus d'infractions commises par des « génies de l'informatique » dans le sens où ils utilisent des techniques complexes ?

« Oui, en plus on a des pirates d'États. On constate que la Corée du Nord, la Russie disposent de ces pirates, qui sont au service de l'État. Ils peuvent collecter des données pour perturber des situations dans un certain nombre de pays. On peut imaginer que certains peuvent également s'amuser et gagner un peu d'argent. »

Question 6ter : Du coup, il y a moins de cas où il s'agit juste de l'usage de pseudonyme sur les réseaux sociaux ?

« C'est un anonymat technique mais quand même de l'usurpation d'identité. D'ailleurs j'ai encore vu récemment un rapport du Centre Cybersécurité Belgique qui met en évidence qu'ils ont reçu un nombre important de témoignages via la fraude au CIO (chef d'entreprise). Là encore une fois, qu'est ce qui se passe ? Le pirate peut se documenter sur les entreprises grâce aux bilans d'entreprise. Ensuite il va sur LinkedIn, il cherche le nom de l'entreprise et là il voit la liste du membre du personnel qui s'est, évidemment, inscrit sur LinkedIn. Là on a la fonction, le nom, le numéro de téléphone, l'adresse mail, etc. Et donc, il va envoyer un message à un membre de la comptabilité ou au patron, en se faisant passer pour le boss : « On a un partenariat qui est en train de se mettre en place avec une structure externe. Je te joins le profil de la structure mais également le contrat qu'on a avec eux. Ils me demandent de faire un versement rapide parce que ... » Et donc, la comptabilité reçoit ça et fait un versement au compte qui n'a rien à voir avec la structure, tout est inventé. »

Question 8 : Est-ce que selon vous les règles d'autorégulation des plateformes sont suffisantes pour encadrer l'usage de pseudonymes et de faux profils ?

« Tout dépend de la façon dont ils peuvent vérifier la création d'un profil, mais je me doute qu'il y en a qui ne font pas toujours ce travail. Il y a tellement de gens qui créent des profils que ce n'est pas toujours évident. Il faut attendre malheureusement le signalement de gens qui sont tombés dans le piège pour qu'eux puissent, à ce moment-là, faire des investigations par rapport à l'origine du profil en question. »

Question 8bis : Ce serait donc extrêmement difficile à faire pour eux, étant donné le nombre d'utilisateurs, de faire ce processus ?

« Oui. Quand on voit les milliards d'utilisateurs de Facebook par exemple. Ce n'est pas toujours facile. En plus Facebook a été victime d'une fuite de données de 700 millions de comptes d'utilisateurs. Je pense maintenant que s'il y a un faux-profil créé avec les données de comptes concernées par une fuite de données, là il y a une vérification. Mais à confirmer. »

Question 9 : Quelle est la place de la victime dans les procédures ?

« La première chose qu'elle doit faire c'est rassembler un maximum de contenu. Je conseille aux gens de faire des captures d'écran des messages, des mails et de les imprimer. Ensuite, elle doit se rendre dans la zone de police locale de son domicile. Et là déposer plainte, si c'est une arnaque par exemple pour escroquerie/arnaque. A ce moment-là, le magistrat reçoit le dossier et consulte l'ensemble des éléments fournis. Et puis alors là il peut prendre contact avec la CCU régionale liée à son arrondissement et leur demander de faire des vérifications dans tel ou tel domaine. A ce moment-là, le magistrat peut également fournir le réquisitoire pour prendre contact avec les structures associées, comme Google, etc. »

Question 10 : Selon vous, quels sont les aspects procéduraux à améliorer au niveau belge ou européen pour favoriser l'identification d'un individu sur les réseaux sociaux ?

« J'ai reçu la visite de Mathieu Michel il y a 15 jours. Et le secrétaire d'État au numérique est en train de travailler sur une révision de la législation de façon à ce que nous puissions, comme nos collègues français, comme nos collègues du Canada, pouvoir, sans réquisitoire, accéder à des données. Il est donc en train de travailler par là avec le Parlement. Il y a une réflexion qui est en cours par rapport à ça. C'est vrai que quand j'ai des contacts avec des collègues des pays que j'évoquais, ils n'ont pas de procédures lourdes, ils prennent contact directement avec l'hébergeur et puis automatiquement ils reçoivent les infos. C'est donc en train de bouger doucement. »

Bibliographie

Législation

Conseil de l'Europe

- Convention de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950, approuvée par la loi du 13 mai 1955, *M.B.*, 19 août 1955.
- Convention du 23 novembre 2001 du Conseil de l'Europe sur la cybercriminalité, signée à Budapest le 23 novembre 2001.
- Rapport explicatif de la convention sur la cybercriminalité du 23 novembre 2001, S.T.C.E. n°185, p. 6 et p. 49.
- Deuxième Protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques, 28 février 2023, S.T.C.E n°224.

Union européenne

- Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *J.O.C.E.*, 23 novembre 1995.
- Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information et notamment du commerce électronique dans le marché intérieur (« Directive sur le commerce électronique »), *J.O.C.E.* no L 178 du 17 juillet 2000.
- Charte des droits fondamentaux de l'Union européenne du 7 décembre 2000, *J.O.C.E.*, 18 décembre 2000.
- Directive 2001/29/CE du Parlement européen et du Conseil du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information, *J.O.C.E.*, n° L 167 du 22.06.2001.
- Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (« Directive vie privée et communications électroniques »), *J.O.U.E.*, 31 juillet 2002.

- Directive 2004/48/CE du Parlement européen et du Conseil du 29 avril 2004 relative aux mesures et procédures visant à assurer le respect des droits de propriété intellectuelle, *J.O.U.E.*, n° L 157 du 30 avril 2004.
- 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, *J.O.U.E.*, 17 décembre 2011.
- 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.
- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la Directive 95/46/CE, *J.O.U.E.*, 27 avril 2016.
- Directive (UE) 2017/541 du Parlement européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil, *J.O.U.E.*, 31 mars 2017.
- Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la Directive 2000/31/CE (« Règlement sur les services numériques »), *J.O.U.E.*, 27 octobre 2022, n° L 277.
- Directive (UE) 2023/1544 du Parlement européen et du Conseil du 12 juillet 2023 établissant des règles harmonisées concernant la désignation d'établissements désignés et de représentants légaux aux fins de l'obtention de preuves électroniques dans le cadre des procédures pénales, *J.O.U.E.*, 28 juillet 2023.
- Règlement (UE) 2023/1543 du Parlement européen et du Conseil du 12 juillet 2023 relatif aux injonctions européennes de production et aux injonctions européennes de conservation concernant les preuves électroniques dans le cadre des procédures pénales et aux fins de l'exécution de peines privatives de liberté prononcées à l'issue d'une procédure pénale, *J.O.U.E.*, 28 juillet 2023.
- Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions, « Les plateformes en ligne et le marché unique numérique – Perspectives et défis pour l'Europe », *COM (2016) 288 final*.
- Résolution du Parlement européen du 15 juin 2017 sur les plateformes en ligne et le marché unique numérique (2016/2276(INI)).

- Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, « Lutter contre le contenu illicite en ligne pour une responsabilité accrue des plateformes en ligne », *COM* (2017) 555 final.
- 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.

Belge

- C.i.cr., articles 46*bis*.
- Const., articles 19 ; 22.
- Code de droit économique, articles XI.334 et XII.17 à 20.
- Loi du 28 novembre 2000 sur la criminalité informatique, *M.B.*, 3 février 2001.
- Projet de loi relative à la criminalité informatique, *Doc. parl.*, ch. repr., sess. ord., 1999-2000, n°50-213/001.
- Loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information, *M.B.*, 17 mars 2003.
- Loi du 10 mai 2007 relative aux aspects civils de la protection des droits de propriété intellectuelle, *M.B.*, 10 mai 2007.
- Loi du 3 août 2012 portant assentiment à la Convention sur la cybercriminalité faite à Budapest le 23 novembre 2001, *M.B.*, 21 novembre 2012.
- 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.
- 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, *Doc. parl.*, Ch. repr., sess. ord., 2015-2016, n°54-1966/1.
- Loi du 22 mai 2017 relative à la décision d'enquête européenne en matière pénale, *M.B.*, 23 avril 2017.
- Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *M.B.*, 5 septembre 2018.

- A.R. du 9 janvier 2003 déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques, *M.B.*, 10 février 2003.

Jurisprudence

Cour européenne des droits de l'homme

- Cour eur. D.H., arrêt *Handyside c. Royaume-Uni*, 7 décembre 1976, n° 5493/72.
- Cour eur. D.H., arrêt *Marckx c. Belgique*, 13 juin 1979, n° 6833/74.
- Cour eur. D.H., arrêt *Niemietz c. Allemagne*, 16 décembre 1992, n°13710/88.
- Cour eur. D.H., arrêt *Ozgur Gundem c. Turquie*, 16 mars 2000, n° 23144/93.
- Cour eur. D.H., arrêt *Pretty c. Royaume-Uni*, 29 avril 2002, n° 2346/02.
- Cour eur. D.H., arrêt *Smirnova c. Russie*, 24 avril 2003, n° 46133/99 et 48183/99.
- Cour eur. D.H., arrêt *Sidabras et Dziautas c. Lituanie*, 27 juillet 2004, n° 55480/00 et 59330/00.
- Cour eur. D.H., arrêt *Muscio c. Italie*, 13 novembre 2007, n° 31358/03.
- Cour eur. D.H., arrêt *K.U. c. Finlande*, 2 décembre 2008, n° 2872/02.
- Cour eur. D.H., arrêt *Glor c. Suisse*, 30 avril 2009, n° 13444/04.
- Cour eur. D.H., arrêt *Delfi AS c. Estonie*, 10 octobre 2013, n°64669/09.
- Cour eur. D.H., arrêt *Delfi AS c. Estonie*, 16 juin 2015, n°64569/09.

Cour de justice de l'Union européenne

- C.J.U.E., arrêt *Productores de Musica de Espana (Promusicae) c. Telefonica de Espana SAU*, 29 janvier 2008, C-275/06.
- C.J.U.E., ordonnance *Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH c. Tele2 Telecommunication GmbH*, 19 février 2009, C-557/07.
- C.J.U.E., arrêt *Bonnier Audio AB e.a. c. Perfect Communication Sweden AB.*, 19 avril 2012, C-461/10.
- C.J.U.E., arrêt *Coty Germany GmbH c. Stadtsparkasse Magdeburg*, 16 juillet 2015, C-580/13.
- C.J.U.E., arrêt *Tobias Mc Fadden c. Sony Music Entertainment Germany GmbH*, 15 septembre 2016, C-484/14.
- C.J.U.E. , arrêt *Mircom c. Telenet BVBA*, 17 juin 2021, C-597/19.

Française

- T.G.I. Paris (réf.), 29 octobre 2007.
- C.A. Paris, 14^e ch., sect. A, 12 décembre 2007, Google Inc / Benetton, Bencom.
- C.A. Paris, 13^e ch., sect. B, 27 avril 2007, Guillemot.
- C.A. Paris, 13^e ch., sect. A, 15 mai 2007, Sebaux.
- C.P.I.J., 7 septembre 1927, *SS Lotus (France/Turquie)*, *C.P.J.I. Rec.*, 1927, Série A, n° 10, pp. 18-19.

Belge

- Cass., (2^e ch.), 18 janvier 2011, R.G. n° P.10.1347.N.
- Cass., 16 juin 2011, *R.D.T.I.*, 2012, p. 69.
- Cass., (2^e ch.), 4 septembre 2012, *T. Strafr.*, 2012/6, p. 464.
- Cass., 19 juin 2013, n° F-20130619-2 (P.12.1150.F).
- Cass., (2^e ch.), 1^{er} décembre 2015, R.G. n° P.13.2082.N.
- Cass., 19 février 2019, R.G. n°P.17.1229.N.
- Gand (3^e ch.), 30 juin 2010, *T. Strafr.*, 2011/22, p. 132.
- Bruxelles (13^e ch.), 12 octobre 2011, *A&M*, 2012/2-3, pp. 238 et 239.
- Anvers (12^e ch.), 20 novembre 2013, *T. Strafr.*, 2014/1, p. 73.
- Anvers, 15 novembre 2017, §5.1.2.1.
- Civ. Bruxelles fr. (réf.), 4 juillet 2022, R.G., n°2022/24/C.
- Corr. Flandre orientale (div. Termonde), 2 mars 2009, *T. Strafr.*, 2009/2, p. 116.

Doctrine

- ADAM A., « Anonymat et faux anonymat : comment identifier et poursuivre les auteurs de contenus haineux sur les réseaux sociaux », in *La régulation des contenus haineux sur les réseaux sociaux*, Anthemis, Limal, 2022, pp. 87-103.
- ARAMAZANI, A., « Le droit à l'oubli et internet », *R.D.T.I.*, 2011/2, n° 43, pp. 34-49.
- BARBRY E., « Le droit de l'Internet est devenu au fil des années un « droit spécial » », *Gaz. Pal.*, 23 octobre 2010, p.14.
- BLANDIN-OBERNESSER A., « Digital Services Act et Digital Markets Act : un nouveau cadre européen pour la régulation des plateformes », in *La politique européenne du numérique* (sous la dir. de BERTRAND B.), 1^e édition, Bruxelles, Bruylant, 2022, pp. 693-702.

- CAMPOLINI P., HERMOYE S. et LEJEUNE F., « Droit d’auteur et contrefaçon dans l’environnement internet : les injonctions contre les intermédiaires », *A&M*, 2017/3, pp. 238-263.
- CAMPOLINI P., CABAY J., BERWETTE M., BIART J. et CROISANT G., « Chronique de législation en droit privé (Deuxième partie) », *J.T.*, 2023/23, n° 6945, pp. 373-381.
- CARRERA S., GONZALEZ FUSTER G., GUILD E. et MILTSILEGAS V., *Acces to Electronic Data by Third-Country Law Enforcement authorities*, Center for European Policy Studies, Bruxelles, 2015. (traduction libre)
- CASTETS-RENARD C., NDIOR V. et RASS-MASSON L., « Introduction », in *Enjeux internationaux des activités numériques : entre logique territoriale des États et la puissance des acteurs privés*, (sous la dir. de CASTETS-RENARD C., NDIOR V. et RASS-MASSON L.), Bruxelles, Larcier, 2020, pp. 9- 18.
- CASTETS-RENARD C., « Titre 2 - Régulation des contenus des plateformes », in *Droit du marché unique numérique et intelligence artificielle*, 1^e édition, Bruxelles, Bruylant, 2020, pp. 151-211.
- CITRON D. K., « Restricting speech to protect it », in *Free speech in the digital age* (sous la dir. de BRISON S.J., GELBER K.), Oxford University Press, 2019, pp. 122-136. (traduction libre)
- CORNU E. et DOCQUIR B., « IV. - Le respect de la vie privée », in *Les réseaux sociaux et le droit* (sous la dir. de SALMON, M.), 1^e édition, Bruxelles, Larcier, 2014, pp. 107-122.
- DE BACKER N., « Le principe de proportionnalité à l’épreuve de la liberté d’expression numérique », *J.E.D.H.*, 2019/4, pp. 256-257.
- DEBIES E., « Comment lutter contre la désinformation sans porter atteinte aux droits fondamentaux et en particulier la protection des données : la recherche d’équilibre opérée par l’Autorité de protection des données (APD) belge dans l’affaire des messages Twitter à propos de l’affaire Benalla – Regard d’une juriste française », *R.D.T.I.*, 2022/2, pp. 89-101.
- DE HERT P. et BOULET G., « Yahoo ! moet meewerken met Belgische procureur », *Juristenkrant*, 2012, n°253, p.8. (traduction libre)
- DERIEUX E. et GRANCHET A., *Réseaux sociaux en ligne : aspects juridiques et déontologiques*, Rueil-Malmaison, Lamy, 2013.
- DE SCHEPPER K., « Cassatie bevestigt: Belgische gerecht kan rechtstreeks gegevens vorderen van Yahoo », *R.A.B.G.*, 2016/7, p. 489-493. (traduction libre)
- DOCQUIR B. « Titre 4 : Responsabilité et sécurité », in *Droit du numérique : contrats, innovation, données et sécurité*, Bruxelles, Larcier, 2018, pp. 565- 615.

- DOCQUIR P.-F, « Chapitre 2. - La confrontation entre droits fondamentaux et puissances privées vue à travers le prisme de la liberté d’expression », in *L'Europe des droits de l'homme à l'heure d'Internet*, Bruxelles, Bruylant, 2019, pp. 75-93.
- DONNAT F., *Droit européen de l'internet : Réseaux, données, services*, Paris, L.G.D.J., 2018.
- DUMORTIER F. et FORGET C., « Criminalité informatique », *R.D.T.I.*, 2017/3-4, n° 68 - 12 novembre 2018, pp. 199-218.
- ELKIN-KOREN N. et PEREL M., « Guardian the Guardians: Content Moderation by Online Intermediaries and the Rule of Law », in *The Oxford Handbook of Online Intermediary Liability*, Oxford University Press, Oxford, 2020, p. 669.
- ENGLEBERT J., « Titre 4 – La liberté d’expression à l’heure de l’Internet », in *Vie privée, liberté d’expression et démocratie dans la société numérique*, Bruxelles, Larcier, 2020, pp. 124-143.
- ERNOTTE F., *Le droit des réseaux sociaux*, Bruxelles, Larcier, 2021.
- FARCY A., « Vie privée et liberté d’expression : application aux publications et « likes » sur Facebook d’un travailleur », *R.D.T.I.*, 2018/2, p. 115-131.
- FRANSSSEN 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*, Bruxelles, Bruylant, 2019, pp. 133-215.
- FORGET C., « La collecte de preuves informatiques en matière pénale », in *Pas de droit sans technologies* (sous la dir. de HENROTTE J.-F., JONGEN F.), Bruxelles, Larcier, 2015, pp. 251-278.
- 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.
- FORGET C. et DUMORTIER F., « La loi du 20 juillet 2022 ou l'art de dissimuler l'obligation de conservation systématique et indifférenciée des métadonnées », *J.T.*, 2023/25, n° 6947, p. 405-413.
- GELBER K. et BRINSON S.J., « Digital dualism and the “speech as thought” paradox », in *Free speech in the digital age* (sous la dir. de BRINSON S.J. et GELBER K.), Oxford University Press, 2019, pp. 12-32. (traduction libre)
- GEORGE F. et HUBIN J., « Les prestataires intermédiaires de la société de l’information face au droit commun de la responsabilité extracontractuelle », *A&M*, 2017/3, pp. 208-237.

- GIACOMETTI M. et MONVILLE P., « 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 M. SALMON), Bruxelles, 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*, Bruxelles, Bruylant, 2019, pp. 287-325.
- GIACOMETTI M., « La récolte transfrontière de preuves électroniques dans le contexte européen. Construction d'un modèle à l'aune d'une nouvelle conception de la souveraineté des États », *A.D.L.*, 2019/3, pp. 423-466.
- GIACOMETTI M., « La récolte de preuves électroniques entre les mains de fournisseurs de services américains : mission impossible pour les autorités en charge des enquêtes dans les États membres de l'Union ? », *J.D.E.*, 2022/2, pp. 42-52.
- GIACOMETTI M., « Partie 2 : La récolte transfrontalière de preuves électronique au moyen d'instruments d'entraide judiciaire. Analyse de la décision d'enquête européenne et des dispositions spécifiques contenues dans la Convention de Budapest, in *La récolte transfrontière de preuves électroniques dans le contexte européen*, 1^e édition, Bruxelles, Bruylant, 2023, pp. 243-457.
- GIACOMETTI M., « Chapitre 2 - La récolte transfrontière de preuves électroniques en droit belge », in *La récolte transfrontière de preuves électroniques dans le contexte européen*, 1^e édition, Bruxelles, Bruylant, 2023, pp. 571-687.
- GOSSE 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.
- HARDOUIN R., « La jurisprudence, les textes et la responsabilité des hébergeurs », *R.L.D.I.*, 2008/39, p. 68.
- HOEBEKE S., MOUFFE B., *Le droit de la presse : presse écrite, presse audiovisuelle, presse électronique*, 3^e édition, Limal, Anthemis, 2012.
- HOUDIJK J., « The e-Commerce Directive and its relation to the proposed Digital Services Act : is the European Union ready for a new digital age ? », in *L'influence du droit européen en droit économique / Cabinet de curiosités pour un juriste passionné – Liber Amicorum Denis Philippe* (sous la dir. de STROWEL A., MINNE G.), 1^e édition, Bruxelles, Larcier, 2022, pp. 745-764. (traduction libre)

- JACQUEMIN, H., « Qui peut obtenir les informations permettant de rechercher et de poursuivre les auteurs d'infractions commises sur les réseaux ? », note sous Cass. (1^{re} ch.), 16 juin 2011. *R.D.T.I.*, (47), pp. 69-81.
- KARAMBIRI Z., « La responsabilité liée aux contenus postés dans les blogs », *R.D.T.I.* 2009/3, n° 36 - 20 octobre 2009, pp. 29-61.
- KELLER D., « Internet Platforms: Observations on Speech, Danger and Money », *Hoover institution's Aegis Paper Series*, 2018, n°1807. (traduction libre)
- KERZMANN L., « L'affaire Yahoo ! ou à qui s'adresse l'obligation de collaboration instaurée par l'article 46bis du Code d'instruction criminelle ? », *R.D.T.I.*, 2011/3, n°44, pp. 116-123.
- KEUP M., « Obtenir une mesure de blocage d'un site Internet contre un fournisseur d'accès à Internet : état des lieux », *R.D.C.-T.B.H.*, 2019/6, pp. 713-722.
- KNOCKAERT M., « Note sous C.J.U.E. (5^e ch.), 17 juin 2021, C-597/19 », *R.D.T.I.*, 2021/3, n° 84, pp. 69-85.
- LARCHE M., « Le Digital Services Act : un pas européen supplémentaire dans la lutte contre l'incitation à la haine et la violence sur les réseaux sociaux », *Rev. Aff. Eur.*, 2021/1, pp. 139-152.
- LEONARD T., « Les réseaux sociaux face à l'exonération de responsabilité des intermédiaires de l'internet : une application délicate », in *Les réseaux sociaux et le droit*, Bruxelles, Éditions Larcier, 2014, pp. 123-150.
- 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.
- LUCAS A., « La responsabilité civile des acteurs de l'Internet », *A&M*, 2001/1, pp. 42-52.
- MARCHADIER F., « Chapitre II - Le web », in *Les nouveaux pouvoirs* (sous la dir. de CAIRE A.-B.), 1^e édition, Bruxelles, Bruylant, 2017, pp. 59-72.
- MICHEL A., « La régulation de la modération des contenus en ligne, une affaire de droits humains ? », *Rev. Trim. D.H.*, 2023/133, p. 41.
- MONTAGNANI M.-L., « Intermediary Liability Regime in the Digital Single Market », in *Questions choisies de droit européen des affaires / Selected Issues in European Business Law* (sous la dir. de VAN CLEYNENBREUGEL P., WILDEMEERSCH J.), 1^e édition, Bruxelles, Bruylant, 2023, pp. 115-131. (traduction libre)
- MONTERO E., « Les responsabilités liées au web 2.0 », *R.D.T.I.*, 2008/32., pp. 363-388.
- MONVILLE, P. et GIACOMETTI, M., « Les fournisseurs d'accès à internet, nouveaux gendarmes de la toile ? », *R.D.T.I.*, 2014/2, n° 55, pp. 68-76.

- MOUFFE, B., *Le droit au mensonge*, Bruxelles, Larcier, 2017.
- PAILLER L., « Chapitre 1 - La garantie du libre accès au réseau social par la vie privée sociale », in *Les réseaux sociaux sur internet et le droit au respect de la vie privée*, 1^e édition, Bruxelles, Larcier, 2012, pp. 27-64.
- POULLET Y., « La lutte contre le racisme et la xénophobie sur internet », *J.T.*, 2006/23, n° 6229, pp. 401-412.
- POULLET Y., « En guise de préface », in *Le droit à la vie privée* (sous la dir. de DOCQUIR B.), Bruxelles, De Boeck-Larcier, 2008, p.10.
- POULLET Y., « Le temps du numérique, le temps du droit et le temps du droit du numérique », in *Guerre et paix* (sous la dir. de ANDRE M.), 1^e édition, Bruxelles, Larcier, 2023, pp. 463-490.
- RICBOURG-ATTAL E., « Section II. - Les acteurs diffuseurs du contenu de l'internet », in *La responsabilité civile des acteurs de l'internet*, 1^e édition, Bruxelles, Larcier, 2014, pp. 165-195.
- TINIERE R., « L'Union européenne et la régulation des plateformes en ligne – À la recherche de la voie du milieu », in *La politique européenne du numérique* (sous la dir. de BERTRAND B.), 1^e édition, Bruxelles, Bruylant, 2022, pp. 703-712.
- TREGUER, F., « Chapitre 8. - Anonymat et chiffrement, composantes essentielles de la liberté de communication », in *L'Europe des droits de l'homme à l'heure d'Internet* (sous la dir. de TERWANGNE C. et VAN ENIS Q.), 1^e édition, Bruxelles, Bruylant, 2019, pp. 295-322.
- TOSZA S., « Cross-border gathering of electronic evidence: mutual legal assistance, its shortcomings and remedies », in *Société numérique et droit pénal: Belgique, France, Europe*, Bruxelles, Bruylant, 2019, pp. 269-285. (traduction libre)
- TURGIS, S., « La coexistence d'internet et des médias traditionnels sous l'angle de la Convention européenne des droits de l'homme », *Rev. Trim. D.H.*, 2013/93, pp. 17-38.
- 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*, Bruxelles, Bruylant. 2019, pp. 93-128.
- UNTERSINGER M., *Anonymat sur internet : comprendre pour protéger sa vie privée*, 1^e édition, Paris, Eyrolles, 2013.
- VANDEZANDE N., « Yahoo ! als operator of vertrekker », note sous Cass., 18 janvier 2011, *A.M.*, 2011, p. 223.

- VAN ENIS Q., « Chapitre 4. - Filtrage et blocage de contenus sur Internet au regard du droit à la liberté d'expression », in *L'Europe des droits de l'homme à l'heure d'Internet* (sous la dir. de TERWANGNE C. et VAN ENIS Q.), 1^e édition, Bruxelles, Bruylant, 2019, p. 146.
- VAN OMMESELAGHE P., « L'autorégulation : rapport de synthèse », in *L'autorégulation*, Bruxelles, Bruylant, 1995, pp. 233 et s.
- WEINSTEIN J., « Cyber harassment and free speech: drawing the line online », in *Free speech in the digital age* (sous la dir. de BRISON S.J., GELBER K.), Oxford University Press, 2019, pp. 52-73. (traduction libre)
- WERKERS, E. et COUDERT, F., « Promusicae versus Telefónica: auteursrecht en recht op privacy in de weegschaal gelegd », *A&M*, 2008/4, pp. 249-263. (traduction libre)

Sources internet

- BICKERT M., « Standards de la Communauté : Facebook publie ses directives internes et élargit son processus de recours aux contenus individuels », disponible sur <https://about.fb.com/fr/news/2018/04/standards-de-la-communaute-facebook-publie-ses-directives-internes-et-elargit-son-processus-de-recours-aux-contenus-individuels/>, consulté le 8 juillet 2023.
- DEGRAUX X., « Réseaux sociaux en Belgique : toutes les statistiques 2023 (étude) », disponible sur <https://www.xavierdegraux.be/reseaux-sociaux-belgique-statistiques-2023-etude>, consulté le 5 juin 2023.
- DELACHARLERY M., « ANONYMAT - Facebook a annoncé qu'il faisait évoluer sa politique d'utilisation des pseudonymes : il sera désormais possible de ne pas utiliser son vrai nom. Ces nouvelles règles s'appliqueront d'ici le mois de décembre. », disponible sur <https://www.tf1info.fr/high-tech/facebook-vous-autorise-enfin-a-avoir-un-pseudo-a-certaines-conditions-1535392.html>, consulté le 3 mai 2022.
- PATRIZIO A., « Qu'est-ce qu'une adresse IP ? », disponible sur <https://www.avast.com/fr-fr/c-what-is-an-ip-address>, consulté le 31 juillet 2023.
- Standards de la communauté Facebook, disponible <https://transparency.fb.com/fr-fr/policies/community-standards>, consulté le 13 juillet 2023.
- Harcèlement et intimidation, disponible sur <https://transparency.fb.com/fr-fr/policies/community-standards/bullying-harassment/>, consulté le 24 juillet 2023.
- Facebook page d'aide : signaler quelque chose, disponible sur <https://www.facebook.com/help/263149623790594>, consulté le 13 juillet 2023.

- Noms autorisés sur Facebook, disponible sur <https://www.facebook.com/help/112146705538576>, consulté le 13 juillet 2023.
- Comment modifier votre profil Twitter, disponible sur <https://help.twitter.com/fr/managing-your-account/change-twitter-handle>, consulté le 5 août 2023.
- Amnesty International Belgique jeunes, « Le cyberharcèlement, on en parle ? », disponible sur <https://jeunes.amnesty.be/jeunes/informe/notre-blog/article/cyberharcèlement>, consulté le 3 mai 2022.
- Amnesty International France, « Harcèlement en ligne : l'impact inquiétant », disponible sur <https://www.amnesty.fr/discriminations/actualites/des-femmes-du-monde-entier-font-etat-de-stress-dangoisse>, consulté le 29 juillet 2023.

Divers

- Avis 2/2002 du Groupe de l'article 29 sur l'utilisation d'identificateurs uniques dans les équipements terminaux de télécommunications, 30 mai 2002, disponible sur https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp58_en.pdf.
- Déclaration sur la liberté de la communication sur Internet *adoptée par le Comité des Ministres lors de la 840e réunion des Délégués des Ministres*, le 28 mai 2003, disponible sur <https://rm.coe.int/16805dfbe1>.
- Rapport juridique 327/2003 de l'Agence espagnole de protection des données (« Carácter de dato personal de la dirección IP »), disponible sur <https://www.aepd.es/es/documento/2003-0327.pdf>.
- Avis 5/2006 du Groupe de l'article 29 sur l'interprétation de la notion de données personnelles, 1er avril 2006, disponible sur https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp122_en.pdf.
- Avis 4/2007 du Groupe de l'article 29 sur le concept de données à caractère personnel, 20 juin 2007, disponible sur https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_fr.pdf.
- Avis 5/2009 du Groupe de l'article 29 sur les réseaux sociaux en ligne, 12 juin 2009, disponible sur https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf.

- Recommandation comité min. n°Rec (2012)4, du Comité des Ministres aux États membres sur la protection des droits de l'homme dans le cadre des services de réseaux sociaux, 4 avril 2012, disponible sur https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805caaad.
- Communiqué de presse de la Commission européenne : « Une Europe adaptée à l'ère du numérique : la Commission propose de nouvelles règles pour les plateformes numériques », 15 décembre 2020 disponible sur https://ec.europa.eu/commission/presscorner/detail/fr/ip_20_2347.
- LEROY M et HAINAUT F., documentaire « #SalePute », (2021), Belgique, RTBF, Proximus, Arte., visionné sur la chaîne Arte sur Youtube le 3 août 2022 (plus disponible en libre accès).

