UCLouvain

Faculté de droit et de criminologie

Cyber-harcèlement : quel cadre juridique pénal pour cette problématique sociétale actuelle ?

Auteur : **Marine Fanourakis**

Promoteur : **Daniel Flore**

Année académique : **2018-2019**

Intitulé du master et de la finalité : **Master en droit, finalité justice civile et pénale**

Plagiat et erreur méthodologique grave

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

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

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

* À ce sujet, voy. notamment **http://www.uclouvain.be/plagiat**.

Remerciements

Je souhaiterais remercier, dans un premier temps, mon promoteur, le Professeur Daniel Flore, pour son encadrement tout au long de la rédaction de ce mémoire.

Je tiens également à témoigner toute ma reconnaissance aux intervenants suivants pour leur contribution essentielle.

Maître Etienne Wéry qui m'a permis d'effectuer un stage à ses côtés dans le domaine des nouvelles technologies de l'information et de la communication. Ce stage a confirmé l'intérêt que je porte aux matières touchant à la cybercriminalité.

Commissaire Olivier Bogaert et Juge d'instruction Philippe Van Linthout pour leur disponibilité et le temps précieux passé à répondre à mes innombrables questions. Leur expérience, tant professionnelle que personnelle, m'ont permis de mieux appréhender la pratique relative au cyber-harcèlement. Leurs judicieux conseils ont contribué à alimenter ma réflexion.

Madame Nathalie Colette-Basecqz, Professeure de droit pénal et du droit de la procédure pénale durant mon bachelier à l'Université de Namur, qui a répondu à mes interrogations et mes doutes.

Finalement, je souhaite adresser mes profonds remerciements à ma famille et mes proches pour leurs encouragements et leur soutien inconditionnel. Je les remercie également pour la relecture de ce mémoire et la correction des imperfections.

« L'évolution des mœurs et des techniques donne matière à de nouvelles formes de délinquance »

cité par

J. CARBONNIER, *Sociologie juridique*, Paris, PUF, 1978, p. 401.

Table des matières

Introduction

« *Je suis le papa de Louise. Et ce que vous voyez là ce sont les messages que ma fille a reçus. Elle recevait des centaines de messages par jour : "même un cochon il veut pas de ton gras", "une photo de tes seins tourne. Salope !", "je te préviens du mal que je vais te faire !", "après avoir sauter, tu seras mieux", "sois mignonne et pends toi", "je me sens moche puis je te vois et ça va mieux", "ce serait cool si tu crevais", "tu feras jamais bander un mec ahah", "va te faire foutre sale garce !"*, etc*. Elle a d'abord essayé de les ignorer en espérant que ça s'arrête, mais ça ne s'est jamais arrêté. Au bout d'un moment c'est devenu insupportable. Aujourd'hui les messages ne la touchent plus. Le 3 septembre 2014, Louise s'est suicidée. Elle avait 16 ans. Elle fait partie des nombreuses victimes du cyber-harcèlement. Pour ma fille c'est trop tard, mais, tous ensemble, nous pouvons faire en sorte que cette tragédie ne se reproduise plus* »[1].

Dans la seconde partie des années 1990, la diffusion à grande échelle des technologies de la communication a fait naître une nouvelle forme de harcèlement, à savoir le harcèlement en ligne ou cyber-harcèlement[2]. Le cyber-harcèlement se distingue du harcèlement « classique » ou moral par l'étendue de la diffusion et la permanence des propos harcelants. Les diverses publications peuvent très rapidement être visionnées par un nombre infini d'utilisateurs et la suppression de ces publications s'avère parfois compliquée car des traces peuvent subsister, par exemple, lorsque des duplications ou copies sont sauvegardées[3]. De plus, le cyber-harcèlement se caractérise par sa continuité permanente. En effet, le monde numérique est devenu accessible à la majorité des citoyens grâce au développement des différentes connections, tant le Wi-Fi que les données mobiles. Cela permet aux utilisateurs d'être connectés à chaque instant[4]. Se pose dès lors la question de la protection des victimes harcelées, vulnérables 24 heures sur 24 et 7 jours sur 7, ne bénéficiant plus d'aucun répit[5]. Par conséquent, ce phénomène récent et grandissant représente un nouvel enjeu pour le législateur qui est celui de trouver un équilibre entre

[1] *Le téléphone de Louise*, une initiative réalisée par *VOO* en partenariat avec la Police Fédérale, disponible sur https://www.letelephonedelouise.com (2 octobre 2018).
[2] K. VAN CLEEMPUT, E. LIEVENS et S. PABIAN, « Een empirisch en juridisch perspectief op cyberpesten: naar een holistische aanpak », *T.J.K.*, 2016/1, p. 7.
[3] D.K. GRIGG, « Cyber-agression : definition and concept of cyberbullying », *Australian Journal of Guidance and Counselling*, 2010, n° 20, p. 143.
[4] N. NIHOUL et S. WATTIER, « La protection de la personne en situation de vulnérabilité par le droit des libertés publiques dans l'environnement numérique », *Vulnérabilités et droits dans l'environnement numérique*, Bruxelles, Larcier, 2018, p. 9.
[5] A. EL ASAM et M. SAMARA, « Cyberbullying and the law : A review of psychological and legal challenges », *Computers in human behavior*, vol. 65, Pergamon, 2016, p. 128.

l'encouragement des libertés publiques et la limitation des comportements « *nocifs, destructeurs, de haine, de harcèlement ou de bafouement des libertés* »[6].

Le phénomène de cyber-harcèlement, pouvant avoir des conséquences gravissimes est en voie d'expansion. Le développement des nouvelles technologies de l'information et de la communication, comme les réseaux sociaux, est devenu un terrain propice aux messages haineux, aux menaces, aux rumeurs, à la divulgation de photos intimes, etc. Plusieurs éléments stimulent une impulsivité qu'il est nécessaire de freiner. Tout d'abord l'absence de contact direct avec la victime ainsi que la rapidité des publications et des échanges anéantissent ou, du moins, réduisent l'impact émotionnel sur le destinateur[7]. Ensuite, la possibilité pour les harceleurs de divulguer anonymement des propos en utilisant un pseudonyme ou un faux nom. Les personnes surfant sur Internet ont souvent la fausse idée que leur anonymat est garanti. Cela a pour conséquence qu'ils font preuve d'une plus grande audace et osent aller plus loin que dans la vie réelle.

Le développement des nouvelles technologies va de pair avec celui de la cybercriminalité. La cybercriminalité est une notion vague et imprécise qu'il est extrêmement délicat de définir. Cela peut être expliqué par son développement continu et son apport grandissant de faits qualifiés ensuite d'infractions par le droit[8]. L'Organisation de coopération et de développement économiques définit largement la cybercriminalité : « *tout comportement illégal ou contraire à l'éthique ou non autorisé qui concerne un traitement automatique de données et/ou une transmission de données* »[9]. La Commission européenne la définit, quant à elle, comme « *toute infraction qui implique l'utilisation des technologies informatiques* »[10]. Le cyber-harcèlement fait donc partie intégrante de la cybercriminalité.

Le droit à la liberté d'expression[11] ainsi que le droit à la confidentialité des communications[12] sont garantis par divers instruments juridiques. Chaque individu jouit

[6] G.A. KAUFMAN, *Liberté d'expression et protection des groupes vulnérables sur Internet*, Paris, L'Harmattan, 2016, p. 10.
[7] B. BEAUDUIN et N. DASNOY, « Relations professeurs/élèves : la ligne rouge : the case of cyberstalking », *New Journal of European Criminal Law*, 2012, n° 3(2), p. 217.
[8] F. DECHAMPS et C. LAMBILOT, *Cybercriminalité : état des lieux*, Limal, Anthemis, 2016, p. 15.
[9] F. DECHAMPS et C. LAMBILOT, « Cybercriminalité : état de la question », *B.S.J.*, 2016/559, p. 8.
[10] Communication de la Commission européenne du 26 janvier 2001 au Conseil, au Parlement, au Comité économique et social, au Comité des régions - Créer une société de l'information plus sûre en renforçant la sécurité des infrastructures de l'information et en luttant contre la cybercriminalité, COM (2000) 890, p. 12.
[11] Art. 10 de la 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, (ci-après abrégée « Conv. E.D.H. ») ; Art. 19 du Pacte international relatif aux droits civils et politiques, fait à New York le 19 décembre 1966, approuvé par la loi du 15 mai 1981, *M.B.*, 6 juillet 1983 ; Art. 11 de la Charte des droits fondamentaux de l'Union européenne, adoptée à Nice le 7 décembre 2000, (ci-après abrégée « Ch. dr. fond. UE ») ; Const., art. 19.
[12] Art. 8 Conv. E.D.H. ; Art. 7 et 8 Ch. dr. fond. UE ; Art. 5 de la Directive 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 (2002/58/CE), *J.O.C.E.*, L-201, 31 juillet 2002 (modifiée par la Directive du Parlement européen et du Conseil du 15 mars 2006 (2006/24/CE), *J.O.U.E.*, L-105, 13 avril 2006, mais abrogée depuis lors et par la Directive du Parlement européen et du Conseil du 25 novembre 2009

de ces deux droits primordiaux, mais ceux-ci ne sont pas absolus. En effet, ils doivent parfois s'estomper lorsqu'il s'agit de respecter la défense de l'ordre, de prévenir des infractions pénales ou de protéger les droits et libertés d'autrui[13]. Les droits et libertés d'autrui sont, notamment, le droit de voir sa réputation ainsi que sa vie privée protégées, le droit de ne pas voir ses informations personnelles divulguées ou le droit de ne pas subir de propos calomnieux, diffamatoires, racistes ou violents[14].

Ce mémoire, composé de trois parties, a pour objet d'introduire le cyber-harcèlement en exposant en quoi celui-ci consiste, en s'interrogeant sur l'état actuel de la législation belge en ce qui concerne les infractions apparentées à celui-ci et en analysant les moyens de recherche dont dispose la justice belge pour récolter la preuve numérique et identifier les auteurs.

La première partie de cet exposé sera dédiée à l'introduction contextuelle du cyber-harcèlement. Après avoir défini celui-ci et ses différentes catégories, nous étudierons ensuite les statistiques contenues dans le Moniteur de sécurité de 2018 publié par la Police Fédérale. Enfin, nous aborderons deux approches européennes concernant les discours de haine en ligne.

Dans la deuxième partie de ce mémoire, nous nous pencherons sur le volet pénal de ce phénomène, incriminant les diverses infractions pouvant s'appliquer dans le cas du cyber-harcèlement. Ces différentes infractions sont régies par la loi du 13 juin 2005 relative aux communications électroniques[15] ainsi que par diverses dispositions du Code pénal. Cependant, il faut être conscient qu'il existe également un volet civil, que nous ne développerons pas. Civilement, plusieurs personnes peuvent voir leur responsabilité engagée telles que l'auteur du cyber-harcèlement, les fournisseurs d'accès, les hébergeurs tenus de la conservation des données fournies par les clients, les parents ainsi que l'école et les instituteurs de l'auteur mineur. Dans la fin de cette partie, nous analyserons le cas spécifique du cyber-harceleur mineur, qui sera déféré devant le tribunal de la jeunesse et bénéficiera, dès lors, de sanctions différentes de celles des adultes.

La troisième et dernière partie de ce travail sera consacrée à la preuve numérique et à l'arsenal de moyens d'action disponibles afin de collecter celle-ci et de procéder à

(2009/136/CE), *J.O.U.E.*, L-337, 18 décembre 2009 ; Const., art. 22 et 29 ; Art. 124 de la loi du 13 juin 2005 relative aux communications électroniques, *M.B.*, 20 juin 2005.

[13] Cour eur. D.H., arrêt K.U. c. Finlande, 2 décembre 2008, req. n° 2872/02, § 49.

[14] C. VILLÉE, K. WINTGENS et S. GÉRARD, « De quelques précautions à l'usage d'Internet », *JDJ*, 2009/6, n° 286, p. 42.

[15] Loi du 13 juin 2005 relative aux communications électroniques, *M.B.*, 20 juin 2005, (ci-après abrégée « loi du 13 juin 2005 »).

l'identification et à la poursuite des auteurs. Nous procéderons, ensuite, à l'analyse des obligations de collaboration pouvant incomber à différents acteurs. Pour finir, nous définirons le rôle à jouer des Federal et Regional Computer Crime Units.

Partie 1. Mise en contexte

Chapitre 1. Définitions

Erling Roland et Elaine Munthe ont défini, en 1989, le harcèlement, dénommé *bullying* en anglais, comme étant « *une violence à long terme, physique ou psychologique, perpétrée par un ou plusieurs agresseurs à l'encontre d'un individu qui est dans l'incapacité de se défendre dans ce contexte précis* »[16]. Dan Olweus, professeur de psychologie norvégien, le définit en 1990 en se référant au harcèlement subi par un élève dans le milieu scolaire : « *un élève est victime de harcèlement lorsqu'il est soumis de façon répétée et à long terme à des comportements agressifs induisant une relation d'asservissement psychologique qui se répète régulièrement amenant des sentiments de peur ou/et de honte* »[17].

Tout comme pour le harcèlement, il n'existe pas de définition unique en ce qui concerne le cyber-harcèlement. D'après Bill Belsey le cyber-harcèlement désigne « *l'utilisation des technologies de l'information et de la communication afin d'adopter de manière délibérée, répétée et agressive, un comportement par un individu ou un groupe dans l'intention de nuire à autrui* »[18]. Les auteurs Dooley, Pyzalski et Cross définissent le cyber-harcèlement comme étant « *une forme de cyber-agression psychologique qui implique la répétition volontaire de nuire à autrui et un déséquilibre de pouvoir comme pour le "bullying" traditionnel* »[19]. Nancy Willard, quant à elle, en donne la définition suivante: « *Cyberbullying is being cruel to others by sending or posting harmful material or engaging in other forms of social cruelty using the Internet or other digital technologies. It has various forms, including direct harassment and indirect activities that are intended to damage the reputation or interfere with the relationships of the student targeted, such as posting harmful material, impersonating the person, disseminating personal information or images, or activities that result in exclusion* »[20].

---

[16] C. BLAYA, « *School bullying* : un type de victimisation en milieu scolaire. Définition et conséquences », *Victimes : du traumatisme à la restauration. Œuvre de justice et victimes*, sous la direction de R. Cario, vol. 2, Paris, L'Harmattan, 2002, p. 127.

[17] D. OLWEUS, *Violences entre élèves, harcèlements et brutalités : Les faits, les solutions*, Collection Pédagogies, Issy-les-Moulineaux, ESF, 1999, cité par R. GUILLOUX, *Situations de harcèlement entre élèves. Comprendre & aider*, 2018, *Retz*, p. 24, disponible sur http://extranet.editis.com/it-yonixweb/images/322/art/doc/8/8d9faf212331353135373531363839323935 31.pdf (26 juillet 2019).

[18] B. BELSEY, « Cyberbullying : An emerging threat to the "always on" generation », 24 mars 2019, disponible sur http://www.billbelsey.com/?cat=13 (26 juillet 2019).

[19] C. BLAYA, *Les ados dans le cyberspace : prises de risque et cyberviolence*, Bruxelles, De Boeck Supérieur, 2013, p. 39.

[20] N. WILLARD, « Cyberbullying legislation and school policies: Where are the boundaries of the "schoolhouse gate" in the new virtual world? », mars 2007, p. 1, disponible sur http://www.embracecivility.org/wp-content/uploadsnew/2012/10/cblegislation.pdf (26 juillet 2019).

Différents critères ont été mis en évidence par Heidi Vandebosch et Katrien Van Cleemput afin qu'un acte soit qualifié de cyber-harcèlement. Cinq critères ont été identifiés sur base des résultats d'enquêtes réalisées auprès de groupes de discussions rassemblant 279 jeunes âgés entre dix et dix-huit ans :

1. L'agresseur doit avoir eu l'intention de blesser (et cela doit avoir été perçu comme tel par la victime) ;
2. Une répétition d'actes négatifs perpétrés en ligne et/ou hors ligne ;
3. Un déséquilibre de pouvoir basé sur des caractéristiques de la vie réelle telles que la force physique ou l'âge et/ou sur des critères liés aux technologies de l'information et de la communication comme le savoir-faire technologique et l'anonymat ;
4. Se produit souvent dans le contexte de groupes sociaux existants (de la vie réelle) ;
5. Vise surtout un individu en particulier[21].

Chapitre 2. Les différentes catégories de cyber-harcèlement

Le harcèlement numérique peut prendre différentes formes qui peuvent être classées en différentes catégories, variant quelque peu selon les auteurs:

- *Flaming* : il s'agit de l'envoi, par les réseaux sociaux, de courts messages très violents.
- *Harassment* : se produit lorsque des messages, offensifs et violents sont envoyés en quantité et de manière répétée.
- *Denigration* : s'entend comme l'ensemble des propos visant à nuire à la réputation de quelqu'un comme par exemple des ragots, des rumeurs ou des calomnies.
- *Impersonation* ou *masquerade* : concerne l'emprunt du pseudonyme d'une personne pour en insulter une autre. L'objectif étant de nuire aux deux personnes.
- *Exclusion* : pratique qui a pour objectif d'écarter volontairement une personne du groupe.
- *Outing* ou *trickery* : constitue l'ensemble des moyens utilisés afin de publier des informations intimes ou confidentielles.
- *Cyberstalking* : méthode consistant à envoyer de multiples messages injurieux ou diffuser méthodiquement et systématiquement des documents gênants[22].

[21] H. VANDEBOSCH et K. VAN CLEEMPUT, « Defining cyberbullying: A qualitative research into the perceptions of youngsters », *CyberPsychology & Behavior*, vol. 11, Mary Ann Liebert, 2008, n° 4, pp. 501 et 502, disponible sur https://pdfs.semanticscholar.org/ee17/16f4ebdef031b324262335625a15d9c9f34b.pdf (27 juillet 2019).
[22] J.-P. BELLON et B. GARDETTE, *Harcèlement et cyberharcèlement à l'école – une souffrance scolaire 2.0*, Collection Pédagogies, Issy-les-Moulineaux, ESF, 2013, pp. 19 et 20.

- *Intimidation* : menacer de manière répétitive dans le but de faire peur et de gagner du pouvoir dans la relation.
- *Sexto* : le fait d'envoyer, répétitivement, des messages à contenu sexuel explicites.
- *Happy slapping* ou vidéo-lynchage: consiste à filmer et diffuser sur les réseaux sociaux, sans le consentement de la victime, des agressions physiques ou des scènes intimes.
- *Slut shaming* : il s'agit d'une discrimination sexiste à des fins de valorisation à l'encontre des filles s'écartant du code de conduite du groupe dominant[23].
- Sites Web de haine : fait de critiquer une personne sur des sites Web consacrés à cet effet ou de créer des tests de popularité ou d'impopularité en ligne[24].
- *Sexting* ou *revenge porn* : concerne la publication sur Internet de photos ou de vidéos d'une personne dénudée ou prenant part à un rapport sexuel. L'auteur de la publication est animé par une volonté de se venger et de nuire[25].

Chapitre 3. Statistiques

Le 3 juillet 2019, la Police Fédérale a publié le Moniteur de sécurité de l'année 2018. Ce Moniteur est le fruit d'une enquête réalisée, de mars à mai 2018, auprès de la population et qui a rassemblé 168 206 participations. L'objectif de cette enquête était notamment d'analyser le sentiment de sécurité ou d'insécurité de la population belge, la tendance des citoyens à porter plainte ainsi que leur appréciation des services de police. Le Moniteur fait mention d'une nette augmentation (14,8% par rapport à 2017) en ce qui concerne la criminalité informatique. Seulement 22% des victimes ayant subi des intimidations et harcèlements via Internet ont déposé plainte, pour ces faits, à la police. Un constat est frappant : au total, environ 200 000 infractions commises par le biais d'Internet n'ont pas fait l'objet d'un signalement. Un défi considérable, pour le futur, consistera à se focaliser sur la prévention et à faciliter le dépôt de plainte dans le but de réduire ce nombre d'infractions non signalées[26].

Par ailleurs, le Moniteur révèle que la tranche d'âge 15-24 ans est celle faisant état du plus grand pourcentage (6,4%) de victimes d'intimidation et de harcèlement par Internet. Ce pourcentage diminue pour les personnes plus âgées, atteignant 1,6% pour la tranche 65

[23] B. HUMBEECK, W. LAHAYE et M. BERGER, *Prévention du harcèlement et des violences scolaires. Prévenir, agir, réagir…*, Louvain-la-Neuve, De Boeck, 2016, p. 35.
[24] M. WALRAVE, M. DEMOULIN, W. HEIRMAN et A. VAN DER PERRE, *Cyberharcèlement : risque du virtuel, impact dans le réel*, Bruxelles, Observatoire des Droits de l'Internet, 2009, pp. 29 et 30.
[25] N. WARTEL, O. MARHRAOUI et C. DE SALLE, « Le cyber-harcèlement des enfants & des adolescents », 2017, *Les études du Centre Jean Gol*, p. 17, disponible sur http://www.cjg.be/wp-content/uploads/2017/03/CJG_ETUDE_Cyber_Harcelement.pdf (25 juillet 2019).
[26] X., « La police fédérale présente le Moniteur de sécurité 2018 », 3 juillet 2019, *Police Fédérale*, disponible sur https://www.police.be/5998/fr/actualites/la-police-federale-presente-le-moniteur-de-securite-2018 (27 juillet 2019).

ans et plus[27]. Inversement, le taux de dépôt de plaintes, en ce qui concerne ces infractions, atteint 33,6% pour les personnes âgées de 65 ans et plus alors qu'il est seulement de 15,9% pour la tranche d'âge 15-24 ans[28].

Comme le souligne le Commissaire à la Computer Crime Unit de la Police Fédérale, Olivier Bogaert, il existe une grande différence entre les statistiques des dossiers ouverts et la réalité[29].

Chapitre 4. D'un point de vue européen

Section 1. Le code de conduite de l'Union européenne du 31 mai 2016 visant à combattre les discours de haine illégaux en ligne

Le 31 mai 2016, la Commission européenne avec l'appui de *Facebook*, *Twitter*, *YouTube* et *Microsoft* a présenté un code de conduite visant à combattre les discours de haine illégaux en ligne. En signant ce code, chacune de ces entreprises a pris l'engagement d'adopter les mesures nécessaires afin de lutter de manière efficace contre les propos appelant à la haine et leur propagation. L'initiative a pour objectif de former le personnel des entreprises afin qu'il puisse traiter les signalements de contenus illicites en moins de 24 heures et que ceux-ci soient supprimés si nécessaire[30]. Ce traitement et le cas échéant, cette suppression, doivent respecter le principe fondamental de la liberté d'expression[31].

Dans ce code de conduite, la Commission définit les engagements que la Commission elle-même, les entreprises des technologies de l'information signataires et les États membres doivent respecter et mettre en œuvre. Parmi ceux-ci :

- Les entreprises signataires doivent mettre en place des procédures d'examen claires et efficaces lors de signalement de la diffusion, au moyen de leurs services, de discours incitant à la haine. Ces procédures doivent permettre une action rapide afin de retirer ou de bloquer l'accès au contenu inapproprié. Des règles ou lignes

[27] X., « Moniteur de sécurité 2018 : Grandes tendances », 3 juillet 2019, *Police Fédérale*, p. 42, disponible sur http://www.moniteurdesecurite.policefederale.be/assets/pdf/2018/reports/Grandes_tendances_Analyses_VMS2018.pdf (27 juillet 2019).
[28] *Ibid*., p. 57, disponible sur http://www.moniteurdesecurite.policefederale.be/assets/pdf/2018/reports/Grandes_tendances_Analyses_VMS2018.pdf (27 juillet 2019).
[29] Voy., *infra,* Annexe 2, p. 84.
[30] M. BRUN, « Lutte contre les discours haineux : le nouveau code de conduite de la Commission », 4 juin 2016, *EU-Logos Athéna*, disponible sur https://www.eu-logos.org/2016/06/04/lutte-contre-les-discours-haineux-le-nouveau-code-de-conduite-de-la-commission/ (3 juillet 2019).
[31] EUROPEAN COMMISSION, « Code of conduct on countering illegal hate speech online », 31 mai 2016, p. 1, disponible sur https://ec.europa.eu/info/sites/info/files/code_of_conduct_on_countering_illegal_hate_speech_online_en.pdf (3 juillet 2019).

directrices doivent être établies afin d'interdire la promotion de comportements incitant à la haine ou à la violence.

- Les signalements doivent être examinés endéans les 24 heures et suivant les règles propres à l'entreprise. Cet examen doit prendre en considération, si nécessaire, la décision-cadre de 2008[32] en confiant cette tâche à des équipes compétentes.
- Les entreprises informatiques doivent informer et conscientiser leurs internautes par rapport aux types de contenus qui ne sont pas autorisés au regard des règles et lignes directrices internes de l'entreprise. Le système de signalement pourrait être utilisé comme instrument afin d'y parvenir.
- Le personnel des entreprises informatiques doit être formé régulièrement afin de s'adapter aux développements actuels de la société. Les entreprises procèdent également à des échanges de points de vue sur les possibilités d'amélioration.
- La coopération entre les entreprises informatiques et les autres plateformes et entreprises actives dans le domaine des médias sociaux doit être intensifiée. Cette coopération doit permettre de renforcer les échanges de bonnes pratiques.
- La Commission européenne, en coordination avec les États membres, encourage l'adhérence d'autres plateformes et entreprises actives dans les médias sociaux aux engagements exposés dans le code de conduite[33].

Dans le courant de l'année 2018, *Google+*, *Instagram*, *Snapchat* et *Dailymotion* ont signé le code de conduite[34]. Nous analyserons ci-après les statistiques relatives à *Google+,* mais uniquement à titre informatif étant donné que la plateforme a été définitivement fermée le 2 avril 2019[35]. Le site français *Jeuxvideo.com* a également adhéré au code en 2019[36].

La quatrième évaluation de ce code, publié en février 2019, confirme le progrès continu concernant le retrait rapide des discours haineux. Le code constitue un instrument efficace afin de lutter contre les discours de haine. Les entreprises informatiques parviennent à traiter la majorité des contenus signalés endéans les 24 heures, atteignant environ 89% des demandes. Cela représente une augmentation significative puisqu'en 2016, le pourcentage était de 40%. Les entreprises des technologies de l'information suppriment,

[32] Décision-cadre du Conseil du 28 novembre 2008 sur la lutte contre certaines formes et manifestations de racisme et de xénophobie au moyen du droit pénal (2008/913/JAI), *J.O.U.E.*, L-328/55, 6 décembre 2008.
[33] EUROPEAN COMMISSION, « Code of conduct on countering illegal hate speech online », 31 mai 2016, pp. 2 et 3, disponible sur https://ec.europa.eu/info/sites/info/files/code_of_conduct_on_countering_illegal_hate_speech_online_en.pdf (3 juillet 2019).
[34] K. KUDRYAVTSEV, « Que fait l'Union européenne contre le cyberharcèlement ? », 20 février 2019, *FranceSoir*, disponible sur http://www.francesoir.fr/politique-monde/que-fait-union-europeenne-contre-le-cyberharcelement (5 juillet 2019).
[35] L. FAURE, « Google+ : Fermeture officielle du réseau social de Google », 3 avril 2019, *IT Social*, disponible sur https://itsocial.fr/actualites/google-annonce-officiellement-processus-de-fermeture-de-google/ (7 juillet 2019).
[36] X., « Haine sur internet : Jeuxvideo.com va se plier au code de conduite de l'UE », 4 février 2019, *RTL Info*, disponible sur https://www.rtl.be/info/magazine/hi-tech/haine-sur-internet-jeuxvideo-com-va-se-plier-au-code-de-conduite-de-l-ue-1097504.aspx (5 juillet 2019).

en moyenne, 72% des propos haineux notifiés. Ce pourcentage est satisfaisant compte tenu du fait que certains contenus signalés ne sont pas illégaux et que seuls ceux-ci peuvent être retirés afin de protéger la liberté d'expression.

Ces statistiques résultent de notifications de contenus haineux présumés illégaux envoyées par 39 organisations appartenant à 26 États membres (excepté le Luxembourg et le Danemark) aux entreprises signataires au cours d'une période de six semaines, s'étalant du 5 novembre au 14 décembre 2018[37]. Ces organisations testent volontairement les réactions des entreprises par rapport aux notifications de discours présumés illégaux et enregistrent leur réponse[38]. Un total de 4392 signalements a été reçu par les entreprises signataires, ce qui représente une augmentation stable. L'entreprise ayant reçu le plus de signalements est *Facebook* (1882), suivie par *Twitter*, *YouTube* (889), *Instagram* (279), *Google+* (28), et *Microsoft* (0). Les organisations volontaires prenant part à l'analyse ont soumis 503 cas, parmi les 4392 signalements, à la police, aux organes du ministère public ou à d'autres autorités nationales[39].

Il est intéressant de comparer le nombre de signalements en fonction des entreprises concernées lors de la première évaluation du code. Cette première évaluation, publiée en décembre 2016, a avancé que *Facebook* était l'entreprise recevant le plus de signalements (270), suivie par *Twitter* (163) et *YouTube* (123). La société *Microsoft* n'en avait quant à elle pas reçu[40].

La quatrième évaluation du code de conduite nous indique également le pourcentage de signalements traités endéans les 24 heures par les entreprises informatiques signataires. Entre le 5 novembre et le 14 décembre 2018, *Facebook* atteint le plus grand pourcentage avec 92,6%, suivi par *Twitter* (88,3%), *YouTube* (83,8%), *Instagram* (77,4%) et enfin *Google+* (60%)[41]. Si on compare ce classement à la première évaluation clôturée en décembre 2016, on constate que *YouTube* occupait la meilleure place. Quant à *Twitter*, il occupait, fin de l'année 2016, la dernière place du classement.

---

[37] V. JOUROVÁ, « *Code of Conduct on countering illegal hate speech online – Results of the fourth monitoring exercise* », février 2019, p. 1, disponible sur https://ec.europa.eu/info/sites/info/files/code_of_conduct_factsheet_7_web.pdf (6 juillet 2019).

[38] V. JOUROVÁ, « *Code of Conduct on countering illegal hate speech online: First results on implementation* », décembre 2016, p. 2, disponible sur http://ec.europa.eu/information_society/newsroom/image/document/2016-50/factsheet-code-conduct-8_40573.pdf (6 juillet 2019).

[39] V. JOUROVÁ, « *Code of Conduct on countering illegal hate speech online – Results of the fourth monitoring exercise* », *op. cit.*, pp. 1 et 2, disponible sur https://ec.europa.eu/info/sites/info/files/code_of_conduct_factsheet_7_web.pdf (6 juillet 2019).

[40] V. JOUROVÁ, « *Code of Conduct on countering illegal hate speech online: First results on implementation* », *op. cit.*, p. 3, disponible sur http://ec.europa.eu/information_society/newsroom/image/document/2016-50/factsheet-code-conduct-8_40573.pdf (6 juillet 2019).

[41] V. JOUROVÁ, « *Code of Conduct on countering illegal hate speech online – Results of the fourth monitoring exercise* », *op. cit.*, p. 2, disponible sur https://ec.europa.eu/info/sites/info/files/code_of_conduct_factsheet_7_web.pdf (6 juillet 2019).

Concernant le pourcentage de suppressions par les entreprises informatiques de contenus illégaux, la quatrième évaluation nous montre que *YouTube* occupe la première place avec 85,4% suivie par *Facebook* (82,4%), *Google+* (80%), *Instagram* (70 ,6%) et enfin *Twitter* (43,5%). Excepté pour *Twitter*, toutes les entreprises font preuve d'une évolution significative depuis la création et l'adhésion au code de conduite. *Twitter* n'atteignant pas la barre des 50%, voit même ses statistiques diminuées entre décembre 2017 (45,7%) et décembre 2018 (43,5%)[42].

En ce qui concerne les motifs des messages haineux qu'on retrouve à travers ces plateformes, la xénophobie occupe la première place avec 17%. L'orientation sexuelle arrive en deuxième position (15,6%) et le racisme à l'encontre des musulmans (13,0%) en troisième position. Notons parmi les autres motifs, la haine à l'encontre des gitans (12,2%), l'antisémitisme (10,1%), les origines ethniques (6,2%), la race (5,3%), la religion (5,2%), la nationalité (5,1%), etc[43].

Concernant la Belgique, 78,9% des contenus signalés ont été supprimés entre le 5 novembre et le 14 décembre 2018 tandis qu'un an plus tôt, ce pourcentage était légèrement plus élevé (83%)[44].

Section 2. La résolution du Parlement européen du 1er mars 2018

La résolution du Parlement européen du 1er mars 2018 sur la situation des droits fondamentaux dans l'Union européenne en 2016 considère que les discours de haine couvrent toutes les formes d'expression, tant celles en ligne que hors ligne. Les discours qualifiés de discours haineux sont ceux qui propagent, encouragent, favorisent ou justifient certaines idées comme, parmi beaucoup d'autres, la haine raciale, les préjugés à l'encontre des caractéristiques génétiques, des opinions politiques ou toute autre opinion, de la fortune, de la naissance, de l'âge. D'après le Parlement européen, de nouvelles formes de médias se développent et de ce fait, simplifient la divulgation de discours de haine en ligne. Ces discours en ligne nécessitent, d'après l'avis du Conseil de l'Europe, de réfléchir et d'agir sur la réglementation et les nouvelles façons de lutter contre cette problématique[45]. Selon cette résolution, il existe un risque consistant à banaliser la hausse de la haine et de la

[42] Voy., *infra,* Annexe 1, Tableau 2, p. 78.
[43] Voy., *infra,* Annexe 1, Tableau 4, p. 81.
[44] Voy., *infra,* Annexe 1, Tableau 3, p. 79.
[45] Résolution du Parlement européen du 1er mars 2018 sur la situation des droits fondamentaux dans l'Union européenne en 2016 (2017/2125(INI)), *J.O.U.E.*, C/129/14, 5 avril 2019, (ci-après abrégée « Résolution du Parlement européen du 1er mars 2018 »), point N, p. 3.

violence à l'égard de la race ou du sexe ainsi que la xénophobie entre les États membres. Cette haine et cette violence peuvent être exprimées par de nombreux moyens comme « *des actes de haine, de fausses nouvelles, des messages anonymes diffusés sur les réseaux sociaux ou d'autres plateformes internet* »[46]. Ces formes d'expression de haine sont favorisées par les réseaux sociaux, mais également par les nombreuses plateformes médiatiques permettant l'anonymat[47].

Afin de lutter contre les discours et propos n'étant pas compatibles avec la législation européenne, il y a lieu, de renforcer la surveillance, la conduite d'enquêtes ainsi que la poursuite, exercées par les autorités compétentes à l'encontre des auteurs. Cette lutte doit néanmoins respecter et protéger la liberté d'expression et le droit à la vie privée[48]. La résolution du Parlement européen insiste sur la nécessité absolue de protéger les droits de l'enfant sur Internet, et particulièrement assurer sa protection contre le cyber-harcèlement[49].

[46] Résolution du Parlement européen du 1er mars 2018, point O, pp. 3 et 4.
[47] Résolution du Parlement européen du 1er mars 2018, point 39, p. 9.
[48] Résolution du Parlement européen du 1er mars 2018, point 46, p. 10.
[49] Résolution du Parlement européen du 1er mars 2018, point 81, p. 14.

Partie 2. Le cadre juridique belge incriminant les faits de cyber-harcèlement

Chapitre 1. Les infractions de harcèlement téléphonique et de harcèlement moral

Section 1. Le harcèlement téléphonique

En 1991, le législateur belge a adopté l'article 114, paragraphe 8, 2°, dans la loi « Belgacom »[50]. Cette disposition a été la première à réglementer le harcèlement téléphonique. Cet article visait à sanctionner toute personne utilisant un réseau ou un service de télécommunications ou d'autres moyens de télécommunications en vue d'importuner son correspondant ou de provoquer des dommages. Toute personne qui commettait cette infraction pouvait être sanctionnée pénalement par une amende de 500 à 50 000 francs et d'un emprisonnement d'un à quatre ans ou d'une de ces peines seulement[51].

Cet article a été abrogé par l'article 155 de la loi du 13 juin 2005. Cette loi opère la transposition, en droit belge, des six directives instituant un nouveau cadre réglementaire européen pour les communications électroniques. Ces directives ont été adoptées par le Parlement et le Conseil de l'Union européenne le 7 mars 2002[52]. La disposition qui est venue lui succéder a été l'article 145, paragraphe 3, 2°, de la loi du 13 juin 2005 précitée. Cet article concernait l'utilisation d'un réseau ou d'un service de communications électroniques ou d'autres moyens de communications électroniques pour importuner son correspondant ou provoquer des dommages. Le non-respect de cette disposition était passible de sanctions pénales consistant en une amende de 500 euros à 50 000 euros et une peine d'emprisonnement d'un an à quatre ans ou une seule de ces peines[53]. Cette disposition a été abrogée par l'article 189 de la loi du 25 avril 2007[54].

[50] Loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques, *M.B.*, 21 mars 1991, (ci-après abrégée « loi du 21 mars 1991 »).
[51] Art. 114, § 8, de la loi du 21 mars 1991.
[52] V. DE SCHRIJVER et A. MISONNE, « Vie du droit. Un nouvel avatar de la législation par référence : la suppression de l'article 114, § 8, de la loi Belgacom », *J.T.*, 2005/34, n° 6196, p. 637.
[53] Art. 145, § 3, de la loi du 13 juin 2005.
[54] Art. 189, 2°, de la loi du 25 avril 2007 portant des dispositions diverses (IV), *M.B.*, 8 mai 2007, (ci-après abrégée « loi du 25 avril 2007 »).

Aujourd'hui, la disposition en vigueur est l'article 145, paragraphe 3*bis*, de la loi du 13 juin 2005[55].

En vertu de cet article, « *est punie d'une amende de 20 euros à 300 euros et d'un emprisonnement de quinze jours à deux ans ou d'une de ces peines seulement la personne qui utilise un réseau ou un service de communications électroniques ou d'autres moyens de communications électroniques afin d'importuner son correspondant ou de provoquer des dommages ainsi que la personne qui installe un appareil quelconque destiné à commettre l'infraction susmentionnée, ainsi que la tentative de commettre celle-ci* ».

Les articles 2, 3° et 5°, de la loi de 2005 définissent les termes « réseau de communications électroniques »[56] et « service de communications électroniques »[57].

Le harcèlement téléphonique ne se limite donc pas au harcèlement réalisé à l'aide d'un téléphone[58]. Il vise également les communications établies à l'aide d'Internet. Pourrait donc constituer du harcèlement téléphonique, des SMS, courriels ou des propos publiés sur des pages Web interactives[59]. Cela permet d'englober la plupart des atteintes en ligne et offre donc une grande protection contre le cyber-harcèlement.

L'infraction suppose la réunion de deux éléments constitutifs.

En ce qui concerne l'élément matériel, celui-ci consiste en l'utilisation d'un réseau ou d'un service de communications électroniques ou d'autres moyens de communications électroniques. Ces moyens de communications ont été définis précédemment. L'élément matériel ne vise donc pas le comportement qu'a adopté l'auteur, mais bien le moyen utilisé par celui-ci. La disposition ne fait pas référence au terme « harcèlement ». Cela a donné lieu à une controverse au sein de la doctrine. Selon certains auteurs, cela implique que la

[55] Art. 189, 3°, de la loi du 25 avril 2007.
[56] Réseau de communications électroniques : « *les systèmes de transmission, et, le cas échéant, les équipements de commutation ou de routage et les autres ressources, y compris les éléments de réseau qui ne sont pas actifs, qui permettent l'acheminement de signaux par câble, par voie hertzienne, par moyen optique ou par d'autres moyens électromagnétiques comprenant les réseaux satellitaires, les réseaux terrestres fixes (avec commutation de circuits ou de paquets, y compris l'Internet) et mobiles, les systèmes utilisant le réseau électrique, dans la mesure où ils sont utilisés pour la transmission de signaux autres que ceux de radiodiffusion et de télévision »,* art. 2, 3°, de la loi du 13 juin 2005.
[57] Service de communications électroniques : « *le service fourni normalement contre rémunération qui consiste entièrement ou principalement en la transmission, en ce compris les opérations de commutation et de routage, de signaux sur des réseaux de communications électroniques, à l'exception (a) des services consistant à fournir un contenu (à l'aide de réseaux et de services de communications électroniques) ou à exercer une responsabilité éditoriale sur ce contenu, à l'exception (b) des services de la société de l'information tels que définis à l'article 2 de loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information qui ne consistent pas entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques et à l'exception (c) des services de la radiodiffusion y compris la télévision »,* art. 2, 5°, de la loi du 13 juin 2005.
[58] N. BANNEUX et L. KERZMANN, « Le mal nommé "harcèlement téléphonique" : chronique des tribulations législatives d'une infraction moderne », *R.D.T.I.*, 2009/1, n° 34, p. 30.
[59] *Ibid*., p. 33.

répétition d'actes litigieux n'est pas une condition nécessaire au harcèlement téléphonique[60]. Selon d'autres auteurs, le harcèlement téléphonique exige une répétition de plusieurs comportements. Ceux-ci s'appuient sur les travaux préparatoires de la loi du 21 mars 1991 selon lesquels il y a lieu de punir les « *appels malicieux qui, par leur répétition, importunent les utilisateurs du téléphone* »[61].

Concernant l'élément moral, un dol spécial est nécessaire, et ce, contrairement au dol requis en cas de harcèlement moral. Il faut que l'auteur ait eu la volonté d'importuner le destinataire des communications électroniques ou de provoquer des dommages. Concernant les dommages, ceux visés par la disposition sont ceux causés au moyen de télécommunications[62] [63]. L'article 145, paragraphe 3*bis*, de la loi du 13 juin 2005 se réfère au terme « correspondant » qui peut être une personne physique ou morale. Cela signifie que l'acte litigieux doit prendre place lors d'un échange ou d'une communication. Il doit donc y avoir une relation directe entre l'auteur du harcèlement et sa victime[64]. Cependant, de nombreux messages insultants ou dénigrants publiés sur les réseaux sociaux ne sont pas adressés de façon directe à la personne dénigrée ou insultée[65].

Un arrêt du Tribunal correctionnel de Turnhout du 16 mai 2012 nous éclaire à propos de l'élément moral requis en cas de harcèlement téléphonique. D'après l'arrêt, « *le dol spécial doit s'apprécier au regard du dessein poursuivi par le prévenu. Il ressort clairement du contenu des messages SMS que le prévenu visait une rencontre avec la mineure, ne laissant d'ailleurs planer aucun doute sur ses intentions. Ces messages révèlent en outre que le prévenu était parfaitement conscient du fait qu'il jouait un jeu dangereux puisqu'il exprimait sa crainte que ses messages SMS ne tombent en de mauvaises mains. Il ressort incontestablement de l'audition ultérieure du prévenu que son but était d'obtenir un rendez-vous avec la jeune fille en dépit de sa minorité et qu'il n'excluait pas que des relations sexuelles aient pu en résulter. Le tribunal estime dès lors que l'élément moral est suffisamment établi dans le chef du prévenu* »[66].

L'article 145, paragraphe 3*bis*, de la loi relative aux communications électroniques n'offre pas une protection contre toutes les formes de cyber-harcèlement compte tenu de la

[60] M. DE RUE, « Le harcèlement », *Les infractions*, vol. 2 : Les infractions contre les personnes, Bruxelles, Larcier, 2010, p. 744 ; A. MASSET et V. BASTIAEN, « La séparation de fait et quelques infractions pénales spécifiques : le harcèlement entre époux », *Séparation de fait. Commentaires pratiques*, Waterloo, Kluwer, 2004, pp. 36 et 37.
[61] Projet de loi portant réforme de certaines entreprises publiques économiques, Exposé des motifs, *Doc. parl.*, Chambre, 1989-1990, n° 47-1287/1, p. 71, 24 septembre 1990.
[62] Projet de loi portant réforme de certaines entreprises publiques économiques, Exposé des motifs, *Doc. parl.*, Chambre, 1989-1990, n° 47-1287/1, p. 71, 24 septembre 1990.
[63] C.A., 10 mai 2006, n° 71/2006.
[64] N. BANNEUX et L. KERZMANN, *op. cit.*, pp. 34 et 35.
[65] N. WARTEL, O. MARHRAOUI et C. DE SALLE, *op. cit.*, p. 39, disponible sur http://www.cjg.be/wp-content/uploads/2017/03/CJG_ETUDE_Cyber_Harcelement.pdf (25 juillet 2019).
[66] Corr. Anvers (div. Turnhout), 16 mai 2012, *T. Strafr.*, 2012/6, pp. 474 à 476, note F.S.

nécessité d'un usage de communications électroniques, d'un dol spécial consistant à importuner son correspondant ou provoquer des dommages ainsi que d'un échange ou d'une communication entre l'auteur et la victime. C'est pourquoi le comportement visé pourrait être incriminé sur base de dispositions contenues dans le Code pénal.

Section 2. Le harcèlement moral

Le harcèlement moral est incriminé par l'article 442*bis* du Code pénal. En vertu du premier alinéa de cet article, « *quiconque aura harcelé une personne alors qu'il savait ou aurait dû savoir qu'il affecterait gravement par ce comportement la tranquillité de la personne visée, sera puni d'une peine d'emprisonnement de quinze jours à deux ans et d'une amende de cinquante euros à trois cents euros, ou de l'une de ces peines seulement* ». La peine est doublée si ces faits sont commis à l'encontre d'une personne vulnérable en raison de l'âge, d'un état de grossesse, d'une maladie, d'une infirmité ou d'une déficience physique ou mentale. La vulnérabilité de la victime doit être apparente ou connue de l'auteur du harcèlement[67].

Le délit suppose la réunion de trois éléments constitutifs.

Premièrement, il faut un comportement harcelant. La disposition légale ne définit pas ce qu'il y a lieu d'entendre par « harcelant ». D'après les travaux préparatoires, cela consiste à importuner un individu, de manière irritante pour celui-ci[68]. D'après Monsieur Barzin, cette notion doit être entendue dans son sens habituel, pouvant évoluer. C'est au juge d'apprécier, au regard des circonstances de l'affaire, la présence ou l'absence de harcèlement[69]. Parmi les circonstances de l'affaire, le juge peut, par exemple, se référer à la nature des relations qu'entretiennent les intéressés, à leur sensibilité, aux conséquences subies dues aux agissements, à la façon dont la société perçoit généralement ce comportement, à la durée de la période délictuelle ainsi qu'au nombre d'actes posés[70]. Malgré que l'élément matériel ne soit dès lors pas légalement défini, la Cour d'arbitrage a, dans son arrêt du 10 mai 2006, conclu à la non-violation du principe de légalité. D'après la Cour, une infraction est définie de manière claire par la loi quand le justiciable a la possibilité de savoir, au moyen du libellé de la disposition pertinente et, si nécessaire, de

[67] C. pén., art. 442*bis*, alinéa 2.
[68] Proposition de loi insérant un article 460*ter* dans le Code pénal en vue d'incriminer le harcèlement, Exposé introductif de M. Landuyt, coauteur de la proposition de loi, *Doc. parl*., Chambre, 1997-1998, n° 49-1046/8, p. 2, 3 juillet 1998.
[69] Proposition de loi insérant un article 460*ter* dans le Code pénal en vue d'incriminer le harcèlement, Discussion des articles et votes, *Doc. parl*., Chambre, 1997-1998, n° 49-1046/8, p. 8, 3 juillet 1998.
[70] Cass. (2e ch.), 20 février 2013, R.G. n° P.12.1629.F, p. 4.

l'interprétation par les juridictions, quels sont les actes et omissions étant de nature à engager sa responsabilité pénale[71].

Lors des travaux préparatoires de la loi, il a été considéré que le harcèlement pouvait résulter d'un acte unique et ne devait pas nécessairement viser une répétition de comportements[72]. Par la suite, la Cour constitutionnelle ainsi que la Cour de cassation ont restreint le champ d'application du délit en affirmant que seule une succession de comportements peut constituer du harcèlement au sens de l'article 442*bis* du Code pénal[73]. Mais, dans son arrêt du 29 octobre 2013, la Cour de cassation, faisant une interprétation extensive de l'infraction de harcèlement, a rompu avec sa jurisprudence antérieure en considérant qu'un seul agissement peut constituer l'infraction de harcèlement. Cet agissement doit, par sa nature incessante ou répétitive, porter gravement atteinte à l'environnement personnel d'autrui. En l'espèce, une vidéo avait été diffusée sur la plateforme de partage *YouTube*. La victime n'aurait visionné celle-ci qu'une seule fois. La diffusion d'une vidéo sur une telle plateforme permet une utilisation répétée et permanente de celle-ci en ce sens qu'un nombre incalculable de personnes, localisées dans le monde entier, peuvent l'entendre ou la visionner[74] [75].

Deuxièmement, le comportement harcelant doit affecter gravement la tranquillité d'une personne physique déterminée. Un lien causal est donc nécessaire entre les agissements et l'atteinte à la tranquillité de la victime. La Cour constitutionnelle considère qu'il n'est pas discriminatoire de considérer qu'une personne morale ne peut pas être victime de harcèlement puisque seule une personne physique peut voir sa tranquillité affective troublée[76] [77]. Par « personne déterminée », la loi exclut de son champ d'application les actes n'ayant pas de destinataires prédéterminés[78]. Dans les travaux parlementaires, des discussions avaient eu lieu quant à l'addition du mot « manifestement » dans la disposition légale. C'est finalement la notion d'atteinte « grave » qui a été retenue. Cette grave atteinte à la tranquillité doit être appréciée objectivement et pas seulement subjectivement[79]. Autrement dit, le juge ne peut se limiter à prendre en considération les

[71] C.A., 10 mai 2006, n° 71/2006, B.5.1 et B.25.1 ; C.A., 14 juin 2006, n° 98/2006, B.5.1 et B.13.4.1.
[72] Proposition de loi insérant un article 460*ter* dans le Code pénal en vue d'incriminer le harcèlement, Amendement, *Doc. parl.*. Chambre, 1997-1998, n° 49-1046/6, p. 2, 9 juin 1998 ; Proposition de loi insérant un article 460*ter* dans le Code pénal en vue d'incriminer le harcèlement, Discussion des articles et votes, *Doc. parl.*, Chambre, 1997-1998, n° 49-1046/8, p. 8, 3 juillet 1998.
[73] C.A., 10 mai 2006, n° 71/2006, B. 6.2. ; Cass. (2e ch.), 21 février 2007, *J.T.*, 2007, p. 262.
[74] Cass. (2e ch.), 29 octobre 2013, R.G. n° P.13.1270.N.
[75] Q. VAN ENIS, « Entre interprétation restrictive du délit de presse et interprétation extensive de l'infraction de harcèlement : un régime en clair-obscur pour la vidéo en ligne ? », *J.T.*, 2014/21, n° 6565, pp. 395 et 396.
[76] C.C., 10 mai 2007, n° 75/2007, B.7.
[77] P. DE HERT, J. MILLEN et A. GROENEN, « Het delict belanging in wetgeving en rechtspraak. Bijna tot redelijke proporties gebracht », *T. Strafr.*, 2008/1, p. 6.
[78] M. DE RUE, *op. cit.*, p. 731.
[79] A. DE NAUW et F. KUTY, *Manuel de droit pénal spécial*, 4e éd., Liège, Wolters Kluwer, 2018, pp. 571 et 572.

seuls effets ressentis subjectivement par la victime[80]. Ces éléments subjectifs doivent être appuyés par, notamment, des témoignages et des pièces médicales prouvant l'affectation de la tranquillité. De plus, comme il a été dit précédemment, le juge doit évaluer la gravité de l'atteinte en se référant aux effets que cela pourrait avoir sur la population ou le milieu concerné[81].

Concernant l'élément moral, un dol général est requis[82]. Il y a lieu d'établir que l'auteur savait ou aurait dû savoir qu'il affecterait gravement, par son comportement, la tranquillité de la victime. Plusieurs questions préjudicielles, mettant en évidence le trop large pouvoir d'appréciation du juge suite à la définition de l'élément moral, ont été posées à la Cour constitutionnelle. La Cour a conclu que l'article 442*bis* du Code pénal était suffisamment précis et prévisible et, par conséquent, que le principe de légalité n'était pas violé. La Cour a rappelé l'importance de vérifier que l'auteur connaissait les conséquences de son comportement, à savoir, l'atteinte grave à la tranquillité de l'intéressé. Afin d'établir cette connaissance, il y a lieu de recourir à des éléments objectifs que l'auteur ne pouvait ignorer. Parmi ces éléments, nous pouvons retrouver les circonstances du harcèlement, la nature des rapports entre l'auteur et la victime, la façon dont la société ou le milieu social concerné perçoit le comportement ainsi que la personnalité du plaignant[83]. Il est requis que l'auteur du comportement ait agi en étant conscient d'adopter un comportement illicite et d'importuner la victime. Le législateur a ainsi exclu l'incrimination du harcèlement involontaire, étant celui réalisé par une personne fermement, mais erronément convaincue de la légitimité de son agissement[84]. Les actes doivent avoir été posés de manière intentionnelle, mais l'intention de nuire ou de perturber la tranquillité d'autrui n'est pas exigée dans le chef de l'auteur[85].

Section 3. Comparaison entre les deux formes de harcèlement à la lumière de la jurisprudence de la Cour constitutionnelle

Après l'adoption par le législateur, en 1991, de l'article 114, paragraphe 8, 2°, dans la « loi Belgacom », l'article 442*bis* a été inséré dans le Code pénal par la loi du 30 octobre 1998[86].

[80] N. COLETTE-BASECQZ, « La responsabilité pénale liée au phénomène du cyberharcèlement et à ses différentes formes d'expression », *Responsabilités et numérique*, Limal, Anthemis, 2018, pp. 40 et 41.
[81] Cass. (2e ch.), 20 février 2013, R.G. n° P.12.1629.F, p. 3.
[82] O. NEDERLANDT et F. VANSILIETTE, « Droit pénal spécial – Les infractions du Code pénal », *Chronique de droit pénal*, Bruxelles, Larcier, 2017, p. 243.
[83] C.A., 10 mai 2006, n° 71/2006 ; C.A., 14 juin 2006, n° 98/2006 ; C.C., 5 mai 2009, n° 76/2009.
[84] A. DE NAUW et F. KUTY, *op. cit.*, pp. 574 à 576.
[85] K. ROSIER, « Le spamming politique : affaire de harcèlement, de prospection et de traitement de données à caractère personnel ? », *Rev. dr. pén. entr.*, 2010/4, pp. 322 et 323.
[86] Loi du 30 octobre 1998 qui insère un article 442bis dans le Code pénal en vue d'incriminer le harcèlement, *M.B.*, 17 décembre 1998.

Dans deux arrêts consécutifs, la Cour d'arbitrage a conclu à l'inconstitutionnalité de la « loi Belgacom », car, selon elle, rien ne pouvait justifier que des peines beaucoup plus lourdes soient applicables au harcèlement électronique par rapport au harcèlement « classique »[87] [88].

L'article 145, paragraphe 3, 2°, de la loi du 13 juin 2005, qui a succédé à l'article 114, paragraphe 8, 2°, de la « loi Belgacom », a fait l'objet, à deux reprises, du même constat d'inconstitutionnalité par la Cour d'arbitrage[89] [90].

Comme dit précédemment, la disposition de référence aujourd'hui est l'article 145, paragraphe 3*bis*, de la loi du 13 juin 2005.

Plusieurs différences peuvent être mises en évidence lors de la comparaison entre le harcèlement « classique » au sens de l'article 442*bis* du Code pénal et le harcèlement téléphonique au sens de l'article 145, paragraphe 3*bis*, de la loi du 13 juin 2005.

La première dissemblance a donné lieu à un arrêt de la Cour constitutionnelle du 22 décembre 2011[91].

Cet arrêt a été rendu à la suite d'une question préjudicielle formulée par le tribunal correctionnel de Charleroi par un jugement du 21 avril 2011. La question était de savoir si l'article 145, paragraphe 3*bis*, de la loi du 13 juin 2005 viole les articles 10 et 11 de la Constitution en ce qu'il crée une double différence de traitement.

Premièrement, car, contrairement à l'article 442*bis* du Code pénal, il ne prévoit pas de demande expresse de la victime comme condition de recevabilité des poursuites.
Deuxièmement, car il érige en incrimination le fait d'importuner un correspondant à l'aide d'un moyen de communication électronique alors qu'il n'existe aucune prévention lorsqu'on importune un tiers à l'aide d'un autre moyen de communication comme par exemple au moyen du courrier postal traditionnel.

La Cour constitutionnelle a répondu par la négative à la question préjudicielle en développant deux arguments principaux afin de justifier la différence de traitement.

[87] C.A., 10 mai 2006, n° 71/2006 ; C.A., 14 juin 2006, n° 98/2006.
[88] F. VANDEVENNE, « Note : le harcèlement de retour à la Cour constitutionnelle », *Rev. Dr. Pén. Crim.,* 2012/7-8, p. 816.
[89] C.A., 28 mars 2007, n° 55/2007 ; C.A., 18 avril 2007, n° 64/2007.
[90] F. VANDEVENNE, *op. cit.*, p. 816.
[91] C.C., 22 décembre 2011, n° 198/2011, note F. Vandevenne, *Rev. Dr. Pén. Crim.,* 2012/7-8, p. 810.

Tout d'abord, la cour énonce que les abus pouvant être commis via l'usage des communications électroniques sont plus importants que ceux pouvant être perpétrés dans d'autres domaines. Alors que l'article 145, paragraphe 3*bis*, de la loi du 13 juin 2005 requiert un élément moral qui est celui de la volonté d'importuner son correspondant, l'article 442*bis* du Code pénal, quant à lui, n'exige pas d'intention. Il requiert uniquement la connaissance que l'auteur avait ou devait avoir des conséquences de son comportement sur la tranquillité de la personne harcelée. Par l'absence d'intention requise, cet article entend prendre en considération les sentiments de la victime et ainsi conditionner la recevabilité des poursuites à la plainte de celle-ci. En raison du dol spécial requis en cas de harcèlement électronique, il est justifié selon la cour que les conditions de recevabilité des poursuites soient plus souples.

Ensuite, suite aux développements techniques importants récemment apparus dans le secteur, il est compréhensible, pour la cour, que le législateur ait voulu punir de manière spécifique les abus commis par voie de communications électroniques. Par conséquent, il n'est pas discriminatoire de soutenir que les auteurs importunant leur correspondant ou provoquant des dommages par d'autres moyens de communication soient punis en vertu de dispositions du droit commun tel que l'article 442*bis* du Code pénal[92] [93].

La loi du 26 mars 2016[94] a abrogé l'alinéa 3 de l'article 442*bis* du Code pénal. Désormais, l'infraction de harcèlement n'est donc plus un délit sur plainte. Le législateur a abrogé cette condition de plainte car cela ne correspondait plus à la réalité sociale. En effet, seule la victime ou, s'agissant d'une personne vulnérable, les établissements d'utilité publique ou les associations visées par l'article 43 de la loi du 26 novembre 2011[95] pouvaient porter plainte. La réaction pénale dépendait uniquement du souhait de la victime d'ester en justice, or, nombreux sont les cas où la victime se suicide, décède préalablement au dépôt de la plainte ou craint de porter plainte, car elle a été fortement intimidée par les faits de harcèlement. Par conséquent, le ministère public pourra, dorénavant, exercer pleinement son monopole de poursuites ainsi que les possibilités qu'il détient de classer sans suite[96]. C'est ainsi que le délit de harcèlement moral s'aligne désormais sur celui du harcèlement téléphonique en ce qui concerne le dépôt d'une plainte.

[92] C.C., 22 décembre 2011, n° 198/2011, note. F. Vandevenne*, Rev. Dr. Pén. Crim.,* 2012/7-8, pp. 810 à 814.
[93] F. VANDEVENNE, *op. cit.*, pp. 818 et 819.
[94] Loi du 26 mars 2016 modifiant l'article 442*bis* du Code pénal, *M.B.*, 5 avril 2016.
[95] Loi du 26 novembre 2011 modifiant et complétant le Code pénal en vue d'incriminer l'abus de la situation de faiblesse des personnes et d'étendre la protection pénale des personnes vulnérables contre la maltraitance, *M.B.*, 23 janvier 2012.
[96] Proposition de loi modifiant le Code pénal en ce qui concerne l'incrimination du harcèlement moral, Discussion des articles et votes, *Doc. parl.*, Chambre, 2015-2016, n° 54-463/3, pp. 8 et 9, 2 mars 2016.

Comme nous l'avons développé précédemment, il existe d'autres différences majeures entre les deux formes de harcèlement. Tout d'abord, le harcèlement téléphonique, contrairement au harcèlement « classique » requiert l'utilisation d'un réseau ou d'un service de communications ou d'autres moyens électroniques. Ensuite, la disposition incriminant le harcèlement téléphonique ne fait référence à un quelconque comportement effectivement harcelant ou à la tranquillité du correspondant effectivement perturbée[97], à l'inverse de l'article 442*bis* du Code pénal précisant que le comportement harcelant doit porter gravement atteinte à la tranquillité de la victime. C'est pourquoi une controverse existe pour la première forme de harcèlement en ce qui concerne la nécessité d'une répétition de plusieurs comportements. Pour le harcèlement moral, la jurisprudence affirmant la nécessité d'une répétition d'actes semblait bien établie jusqu'à l'arrêt de la Cour de cassation du 29 octobre 2013. Dans cet arrêt, la cour a admis qu'un seul agissement puisse constituer du harcèlement de par sa nature répétitive ou incessante. En ce qui concerne la victime, il doit s'agir du correspondant du harceleur, personne physique ou morale, dans le cas du harcèlement téléphonique alors que la victime doit être une personne physique déterminée dans le cadre du harcèlement moral. Enfin, concernant l'élément moral, un dol spécial consistant en la volonté d'importuner le destinataire des communications électroniques ou de provoquer des dommages doit exister pour le harcèlement téléphonique. En cas de harcèlement « classique », il faut établir que l'auteur savait ou aurait dû savoir qu'il affecterait gravement, par son comportement, la tranquillité de la victime.

Chapitre 2. Le concours idéal d'infractions et les autres infractions du Code pénal susceptibles de s'appliquer au cyber-harcèlement

Section 1. Le concours idéal d'infractions

Fréquemment, dans le cadre d'un phénomène de cyber-harcèlement, plusieurs comportements sont observés et peuvent constituer un concours idéal d'infractions[98]. Un concours idéal d'infractions « *est soit un fait unique constitutif de diverses infractions, soit un complexe de faits caractérisé par l'unité d'intention dans le chef de l'agent* »[99].

[97] E. DELHAISE, « Le suicide de Madison : enfin une prise de conscience en matière de harcèlement ? », 22 avril 2016, *Justice en ligne*, disponible sur http://www.justice-en-ligne.be/article861.html (1er août 2019).
[98] N. COLETTE-BASECQZ, « La protection pénale des personnes vulnérables dans l'environnement numérique », *Vulnérabilités et droits dans l'environnement numérique*, Bruxelles, Larcier, 2018, p. 158.
[99] F. KUTY, « Le concours idéal d'infractions par unité d'intention ou de réalisation », *Principes généraux du droit pénal belge*, tome IV : La peine, Bruxelles, Larcier, 2017, p. 931.

Conformément à l'article 65, alinéa premier, du Code pénal, « *lorsqu'un même fait constitue plusieurs infractions ou lorsque différentes infractions soumises simultanément au même juge du fonds constituent la manifestation successive et continue de la même intention délictueuse, la peine la plus forte sera seule prononcée* ».

Par exemple, lorsque les éléments constitutifs du harcèlement téléphonique rencontrent également ceux du harcèlement moral, un même comportement constitue, dès lors, plusieurs infractions[100]. Un autre cas d'application fréquent dans le cadre du cyber-harcèlement est la commission par un auteur, animé d'une même intention délictueuse, de plusieurs infractions comme par exemple la publication de propos injurieux, l'envoi de menaces, la calomnie, etc.

Section 2. Analyse non exhaustive des différentes infractions pouvant s'apparenter au cyber-harcèlement

De nombreuses infractions sont susceptibles d'être apparentées au cyber-harcèlement. En voici une liste non exhaustive : les menaces (article 327 du Code pénal), le *grooming* et la cyberprédation (articles 337*ter*, article 337*quater* et article 433*bis*/1 du Code pénal), le voyeurisme, la diffusion d'enregistrements issus du voyeurisme et le *revenge porn* (article 371/1 du Code pénal), le traitement dégradant (article 417*quinquies* du Code pénal), la calomnie et la diffamation (articles 443 et 444 du Code pénal), les injures (article 448 du Code pénal), etc. Dans cette étude, nous développerons uniquement les infractions récentes ou ayant fait l'objet d'un revirement jurisprudentiel récent.

1. La cyberprédation et le grooming

Alors que les articles 377*ter* et 377*quater* du Code pénal incriminent l'infraction de *grooming*, l'article 433*bis*/1 du même Code incrimine celle de cyberprédation. Les dispositions relatives au *grooming* ont été, sous une impulsion européenne[101], insérées dans le Code pénal par la loi du 10 avril 2014 relative à la protection des mineurs contre la sollicitation à des fins de perpétration d'infractions à caractère sexuel[102]. Quant à la

[100] N. COLETTE-BASECQZ, « La responsabilité pénale liée au phénomène du cyberharcèlement et à ses différentes formes d'expression », *op. cit.*, p. 58.
[101] Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels, signée à Lanzarote le 25 octobre 2007, *S.T.C.E.*, n° 201 ; Directive du Parlement européen et du Conseil 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 (2011/93/UE), *J.O.U.E.*, L-335/1, 17 décembre 2011.
[102] Loi du 10 avril 2014 relative à la protection des mineurs contre la sollicitation à des fins de perpétration d'infractions à caractère sexuel, *M.B.*, 30 avril 2014.

cyberprédation, l'article 433*bis*/1 a été inséré dans le Code pénal par la loi du 10 avril 2014 modifiant le Code pénal en vue de protéger les enfants contre les cyberprédateurs[103].

En vertu de l'article 377*ter*, « *dans les cas prévus par le présent chapitre ou par les chapitres VI et VII du présent titre, le minimum des peines portées par les articles concernés est doublé s'il s'agit d'un emprisonnement, et augmenté de deux ans s'il s'agit de la réclusion, lorsque le crime ou le délit a été commis à l'encontre d'un mineur de moins de seize ans accomplis et que préalablement à ce crime ou à ce délit, l'auteur avait sollicité ce mineur dans l'intention de commettre ultérieurement les faits visés au présent chapitre ou aux chapitres VI et VII du présent titre. […]* ».

Selon l'article 377*quater*, « *la personne majeure qui, par le biais des technologies de l'information et de la communication, propose une rencontre à un mineur de moins de seize ans accomplis dans l'intention de commettre une infraction visée au présent chapitre ou aux chapitres VI et VII du présent titre, sera punie d'un emprisonnement d'un an à cinq ans, si cette proposition a été suivie d'actes matériels conduisant à ladite rencontre* ».

Enfin, l'article 433*bis*/1 énonce que « *sera puni d'un emprisonnement de trois mois à cinq ans, la personne majeure qui communique par le biais des technologies de l'information et de la communication avec un mineur avéré ou supposé, et ce en vue de faciliter la perpétration à son égard d'un crime ou d'un délit :*

1° s'il a dissimulé ou menti sur son identité ou son âge ou sa qualité;

2° s'il a insisté sur la discrétion à observer quant à leurs échanges;

3° s'il a offert ou fait miroiter un cadeau ou un avantage quelconque;

4° s'il a usé de toute autre manœuvre ».

Le terme « *grooming* » correspond à la phase de planification ou de manipulation, à l'aide de communications électroniques, dans le but de commettre, au détriment de la victime, des actes à caractère sexuel[104] [105]. Le *grooming* suppose une proposition de rencontre au moyen des technologies de l'information et de la communication entre un individu majeur et une personne de moins de seize ans accomplis. Cette proposition doit avoir été émise en vue de perpétrer une ou plusieurs des infractions suivantes : voyeurisme, attentat à la

[103] Loi du 10 avril 2014 modifiant le Code pénal en vue de protéger les enfants contre les cyberprédateurs, *M.B.*, 30 avril 2014.

[104] Proposition de loi modifiant le Code pénal en vue de garantir la protection pénale des enfants contre le « *grooming* » (mise en confiance à des fins d'abus sexuel), Auditions, *Doc. parl.*, Sénat, 2013-2014, n° 5-1823/4, p. 4, 26 février 2014.

[105] O. LEROUX, « Criminalité informatique aspécifique », *Les infractions, 2e* éd., vol. 1 : Les infractions contre les biens, Bruxelles, Larcier, 2016, p. 522.

pudeur, viol, corruption à la jeunesse, prostitution et/ou outrage publics aux bonnes mœurs.

L'article 377q*uater* incrimine spécifiquement la proposition suivie d'actes matériels menant à la rencontre[106]. La loi ne requiert pas que la rencontre, ni que l'une des infractions visée aux articles 372 à 389 du Code pénal aient effectivement eu lieu. Les seules conversations à caractère sexuel sont donc exclues du champ d'application de la disposition. L'auteur doit dès lors avoir mis en place les moyens nécessaires afin que la rencontre se concrétise et doit être animé d'un dol spécial à caractère sexuel, c'est-à-dire qu'il ait la volonté que la rencontre prenne place et l'intention de commettre un abus physique sur le mineur[107]. Généralement, les auteurs veillent à préparer leur victime « *en nouant un lien de confiance, en accordant à l'enfant une attention privilégiée, en instaurant le secret puis en repoussant progressivement leurs limites. Cela leur évite de devoir recourir aux formes plus explicites de pression, de violence ou de force, ce qui leur permet de prolonger l'abus beaucoup plus longtemps. L'enfant est tellement manipulé psychologiquement qu'il ne veut ou n'ose pas dénoncer l'auteur, qu'il ne peut déceler l'abus ou qu'il se sent personnellement responsable de l'abus* »[108].

Les *groomers* utilisent régulièrement des outils informatiques tels que les *chats* publics et privés, les réseaux sociaux, les blogs, les plateformes de jeux ainsi que l'utilisation de la webcam, et ce, à partir de leur domicile en utilisant le Wi-Fi non sécurisé d'un voisin ou des cybercafés. Ils procèdent généralement seuls en prenant l'identité d'un jeune. Ils communiquent, d'abord avec un langage normal qui se sexualise par la suite, avec l'enfant, choisi pour sa vulnérabilité et non surveillé par ses parents lorsqu'il surfe sur Internet[109]. En ce qui concerne les moyens mis en place par l'auteur, les travaux parlementaires citent, à titre d'exemple, le fait qu'il se soit réellement présenté au lieu convenu, qu'il ait déjà acheté des billets de train ou des tickets de cinéma ou qu'il ait demandé à prendre congé pour le jour de la rencontre[110].

L'article 377*ter*, quant à lui, prévoit une circonstance aggravante subjective. Elle consiste en la sollicitation, par la personne majeure, du mineur, dans l'intention de commettre l'une

[106] C. FORGET et F. DUMORTIER, « Criminalité informatique », *R.D.T.I.,* 2015/2-3, n° 59-60, p. 120.
[107] O. LEROUX, « Criminalité informatique aspécifique », *op. cit*., p. 523.
[108] Proposition de loi modifiant le Code pénal en vue de garantir la protection pénale des enfants contre le « *grooming* » (mise en confiance à des fins d'abus sexuel), Exposé introductif de Mme Cindy Franssen, Auteure principale de la proposition de loi, *Doc. parl.*, Sénat, 2013-2014, n° 5-1823/4, p. 2, 26 février 2014.
[109] Proposition de loi modifiant le Code pénal en vue de garantir la protection pénale des enfants contre le « *grooming* » (mise en confiance à des fins d'abus sexuel), Auditions, *Doc. parl*., Sénat, 2013-2014, n° 5-1823/4, p. 6, 26 février 2014.
[110] Proposition de loi modifiant le Code pénal en vue de garantir la protection pénale des enfants contre le « *grooming* » (mise en confiance à des fins d'abus sexuel), Auditions, *Doc. parl*., Sénat, 2013-2014, n° 5-1823/4, pp. 16 et 17, 26 février 2014.

des infractions visées aux articles 372 à 389 du Code pénal. Cette sollicitation entraîne un affaiblissement des mécanismes de défense du mineur[111]. Cette circonstance aggravante vise aussi bien le démarchage effectué sur Internet que la prédation réalisée dans le monde réel, contrairement à l'article 377*quater* qui se limite au seul *grooming* en ligne. Ce démarchage ou cette prédation a pour but de piéger le mineur de moins de seize ans accomplis et précède la commission d'infractions de mœurs à son égard[112].

L'infraction de cyberprédation est, quant à elle, prescrite de manière plus large. En effet, contrairement au *grooming*, elle ne se limite pas aux infractions à caractère sexuel[113]. De plus, elle n'exige pas que l'auteur ait formulé une proposition de rencontre. La cyberprédation suppose une communication via une technologie de l'information et de la communication entre une personne majeure et une personne mineure avérée ou une personne majeure que l'auteur croyait mineure. En ce qui concerne l'élément moral, un dol spécial est requis et consiste en l'intention du majeur d'entrer en contact avec le mineur dans le but de faciliter la commission d'un crime ou d'un délit à son encontre[114]. La rencontre ultérieure à la communication n'est pas nécessaire. Cependant, il est requis que l'auteur ait usé de manœuvres frauduleuses en vue de faciliter la commission d'une infraction à l'égard du mineur[115]. Nous trouvons la liste des manœuvres frauduleuses dans l'article 433*bis*/1, mais celle-ci n'est ni cumulative ni exhaustive[116]. Un acte isolé ne suffit pas. Seule une pluralité d'actes se prolongeant dans le temps afin d'abuser de la faiblesse d'un mineur peut constituer de la cyberprédation[117].

2. Le voyeurisme, la diffusion d'enregistrements provenant de celui-ci et le revenge porn

La loi du 1er février 2016[118] a inséré, dans le Code pénal, l'article 371/1. Au départ, la proposition de loi du 10 décembre 2014[119] avait pour but de procéder à la modification et à l'élargissement de l'incrimination de l'infraction d'attentat à la pudeur[120]. Mais, dans deux

[111] O. LEROUX, « Criminalité informatique », X., *Postal Mémorialis - Lexique du droit pénal et des lois spéciales*, Waterloo, Kluwer, 2014, p. C362/38.
[112] O. LEROUX, « Criminalité informatique aspécifique », *op. cit.*, pp. 523 et 524.
[113] N. COLETTE-BASECQZ, « La protection pénale des personnes vulnérables dans l'environnement numérique », *op. cit.*, p. 156.
[114] O. LEROUX, « Criminalité informatique aspécifique », *op. cit.*, pp. 524 et 525.
[115] C. FORGET et F. DUMORTIER, *op. cit.*, p. 121.
[116] Projet de loi modifiant le Code pénal en vue de protéger les enfants contre les cyberprédateurs, Discussion des articles et votes, *Doc. parl.*, Chambre, 2013-2014, n° 53-3450/2, p. 6, 24 mars 2014.
[117] Proposition de loi modifiant le Code pénal en vue de protéger les enfants contre les cyberprédateurs, Discussion des articles, *Doc. parl.*, Sénat, 2013-2014, n° 5-2253/3, p. 8, 26 février 2014.
[118] Loi du 1er février 2016 modifiant diverses dispositions en ce qui concerne l'attentat à la pudeur et le voyeurisme, *M.B.*, 19 février 2016.
[119] Proposition de loi modifiant le Code pénal en ce qui concerne l'incrimination de l'attentat à la pudeur, *Doc. parl.*, Chambre, 2014-2015, n° 54-699/1, 10 décembre 2014.
[120] M. TÖLLER, « Revenge porn ou vengeance pornographique », *R.D.T.I.*, 2018/2, n° 71, p. 88.

arrêts successifs[121], la Cour de cassation a considéré que le fait de filmer une personne s'adonnant à une relation sexuelle consentie ou une personne dénudée, à son insu et sans son consentement, ne constituait pas un attentat à la pudeur. C'est à la suite de ces arrêts que le législateur a décidé d'instaurer une incrimination autonome de voyeurisme[122] [123].

Conformément à l'article 371/1, alinéa premier, 1°, du Code pénal, une sanction pénale consistant en un emprisonnement de six mois à cinq ans pourra être infligée à toute personne qui a « *observé ou fait observer une personne ou en aura réalisé ou fait réaliser un enregistrement visuel ou audio,*

- directement ou par un moyen technique ou autre,

- sans l'autorisation de cette personne ou à son insu,

- alors que celle-ci était dénudée ou se livrait à une activité sexuelle explicite, et

- alors qu'elle se trouvait dans des circonstances où elle pouvait raisonnablement considérer qu'il ne serait pas porté atteinte à sa vie privée ».

Dès lors, les faits cités précédemment dont la Cour de cassation a eu à connaître pourraient clairement être incriminés sur base de cette disposition[124].

L'article 371/1, alinéa premier, 2°, du Code pénal, quant à lui, punit de la même façon quiconque ayant « *montré, rendu accessible ou diffusé l'enregistrement visuel ou audio d'une personne dénudée ou se livrant à une activité sexuelle explicite, sans son accord ou à son insu, même si cette personne a consenti à sa réalisation* ». Cette disposition est dès lors applicable au cas spécifique du *revenge porn*. Le *revenge porn* ou, également appelé, vengeance pornographique, est couramment défini comme étant « *le fait de diffuser, sans le consentement de la victime, des photos ou des vidéos à caractère sexuel de l'intéressé(e), réalisées avec son consentement, afin de nuire à sa réputation dans le cadre d'une vengeance à la suite, par exemple, d'une rupture* »[125].

Partant de cette définition, ce qui diffère entre la diffusion des contenus visés au premier point de l'article et le *revenge porn* est le consentement de la victime à la réalisation de ces contenus, non présent dans le premier cas. En effet, le *revenge porn* suppose l'application de l'article 371/1, alinéa premier, 2°, indépendamment de l'article 371/1, alinéa premier, 1°, qui concerne le voyeurisme au sens strict[126].

---

[121] Cass. (2e ch.), 27 novembre 2013, R.G. n° P.13.0714.F ; Cass. (2e ch.), 31 mars 2015, R.G. n° P.14.0293.N.
[122] Proposition de loi modifiant le Code pénal en ce qui concerne l'incrimination de l'attentat à la pudeur, Amendement, *Doc. parl.*, Chambre, 2014-2015, n° 54-699/2, pp. 3 à 5, 15 juillet 2015.
[123] M. TÖLLER, *op. cit.*, p. 88.
[124] *Ibid.*, p. 90.
[125] *Ibid.*, p. 87.
[126] *Ibid.*, p. 90.

Les éléments matériels constitutifs de cet article 371/1, alinéa premier, 2° sont donc les suivants :

- montrer, rendre accessible ou diffuser : il suffit qu'une seule personne, autre que l'auteur ou la victime, ait potentiellement accès au contenu. Cette notion de diffusion est dès lors beaucoup plus large que celle de publicité contenue dans l'article 444 du Code pénal que nous analyserons ci-après[127] ;
- un enregistrement visuel ou audio : doit s'entendre largement et vise tout enregistrement photographique, filmé, vidéo, audio ou autre, réalisé à l'aide de n'importe quel moyen ;
- d'une personne dénudée ou se livrant à une activité sexuelle explicite : d'après les travaux préparatoires, il y a lieu d'entendre par « personne dénudée » celle qui « *exhibe une partie de son corps qui, sur base des normes sociales actuelles et de la conscience collective de la pudeur, aurait été gardée couverte si la personne avait su qu'elle était épiée ou filmée sans son autorisation* »[128]. Cette définition pourrait être affinée afin d'être applicable au *revenge porn* en ajoutant « *ou que cet enregistrement, réalisé avec son autorisation, était diffusé* »[129] ;
- sans disposer de son accord ou à son insu ; cela concerne bien évidemment la diffusion de l'enregistrement.

Dans le cas spécifique du *revenge porn*, l'élément constitutif du consentement de la victime à la réalisation de l'enregistrement visuel ou audio peut être ajouté.

Aucune référence n'est faite à l'élément moral. Par déduction, cette disposition requiert l'existence d'un dol général, c'est-à-dire que l'auteur ait agi consciemment et volontairement[130].

Deux circonstances aggravantes sont prévues dans le texte. La première prévoit une peine de réclusion de cinq à dix ans lorsque les faits ont été commis sur ou à l'aide d'un mineur âgé de plus de seize ans accomplis[131]. Lorsque le mineur a moins de seize ans accomplis, le coupable peut se voir infliger une peine de réclusion allant de dix à quinze ans[132]. D'autres circonstances aggravantes prévues aux articles 377, 377*bis* et 377*ter*[133] du Code pénal peuvent également s'appliquer.

[127] *Ibid*., pp. 91 et 92.
[128] Proposition de loi modifiant le Code pénal en ce qui concerne l'incrimination de l'attentat à la pudeur, Amendement, *Doc. parl*., Chambre, 2015-2016, n° 54-699/3, p. 5, 27 novembre 2015.
[129] M. TÖLLER, *op. cit*., p. 93.
[130] *Ibid*., p. 90.
[131] C. pén., art. 371/1, alinéa 2.
[132] C. pén., art. 371/1, alinéa 3.
[133] Voy., *supra*, Partie 2, Chapitre 2, Section 2, pp. 24 à 25.

3. Les atteintes à l'honneur en lien avec le délit de presse

L'article 443 du Code pénal incrimine les infractions de diffamation et de calomnie. Conformément à cette disposition, « *celui qui, dans les cas ci-après indiqués, a méchamment imputé à une personne un fait précis qui est de nature à porter atteinte à l'honneur de cette personne ou à l'exposer au mépris public, et dont la preuve légale n'est pas rapportée, est coupable de calomnie lorsque la loi admet la preuve du fait imputé, et de diffamation lorsque la loi n'admet pas cette preuve* ».

Deux éléments constitutifs de ces infractions méritent d'être éclaircis. Concernant l'élément moral, un dol spécial est nécessaire. L'auteur doit avoir été animé d'une intention coupable, d'une intention de nuire à la victime[134]. Une autre condition requise est celle de la publicité, contenue à l'article 444 du Code pénal. Il peut s'agir d'imputations verbales[135] ou d'imputations écrites visant notamment « *des écrits imprimés ou non, des images ou des emblèmes affichés, distribués ou vendus, mis en vente ou exposés aux regards du public* »[136] ainsi que « *des écrits non rendus publics, mais adressés ou communiqués à plusieurs personnes* »[137]. Ainsi, les imputations faites par voie d'Internet peuvent également être comprises dans la notion de publicité au sens de l'article 444 du Code pénal. Par exemple, cette condition sera aisément remplie lorsqu'un commentaire ou un tweet dénigrant sera publié par le profil public *Facebook* ou *Twitter* d'un utilisateur[138]. Il sera également satisfait à cette condition dans le cas de forums de discussion[139]. Par contre, lorsque les propos sont publiés au moyen d'un profil privé ou partiellement privé n'autorisant l'accès qu'à un certain nombre d'amis, il y aura lieu d'analyser la condition de publicité au regard de l'étendue du cercle d'individus y ayant accès : « *plus ce cercle sera restreint, plus il sera difficile d'établir le caractère public* »[140]. Néanmoins, il est nécessaire de prendre en considération les interactions en cascade générées par les réseaux sociaux, permettant de relayer facilement les informations[141].

L'auteur de ces infractions se verra infliger une peine d'emprisonnement de huit jours à un an et une amende de vingt-six à deux cents euros[142].

---

[134] F. JONGEN et A. STROWEL, « Droit à l'honneur et à la réputation », *Droit des médias et de la communication*, Bruxelles, Larcier, 2017, p. 455.
[135] C. pén., art. 444, alinéas 2, 3 et 4.
[136] C. pén., art. 444, alinéa 5.
[137] C. pén., art. 444, alinéa 6.
[138] M. GIACOMETTI et P. MONVILLE, « Réseaux sociaux, anonymat et faux profils : vrais problèmes en droit pénal et de la procédure pénale », *Les réseaux sociaux et le droit*, sous la direction de M. Salmon, Bruxelles, Larcier, 2014, p. 182.
[139] Corr. Bruxelles, 22 décembre 1999, *A.M.*, 2000, p. 134 (confirmé par Bruxelles (11e ch.), 27 juin 2000, *A.M.*, 2001/1, p. 142), cité par M. GIACOMETTI et P. MONVILLE, *op. cit.*, p. 182.
[140] *Ibid.*, pp. 182 et 183.
[141] *Ibid.*, p. 183.
[142] C. pén., art. 444, alinéa 1er.

Concernant les injures, celles-ci sont incriminées par l'article 448, alinéa premier, du Code pénal. En vertu de cette disposition, « *quiconque aura injurié une personne soit par des faits, soit par des écrits, images ou emblèmes, dans l'une des circonstances indiquées à l'article 444, sera puni d'un emprisonnement de huit jours à deux mois et d'une amende de vingt-six euros à cinq cents euros, ou d'une de ces peines seulement* ». Les conditions de publicité et d'intention méchante dans le chef de l'auteur doivent également être remplies pour cette infraction[143]. Contrairement à la diffamation ou à la calomnie, les injures ne doivent pas porter sur un fait précis[144].

Lorsque le mobile du délit est discriminatoire, l'article 453*bis* du Code pénal prévoit que le minimum des peines correctionnelles prévu pour ces infractions pourra être doublé. Il est également intéressant de préciser que ces trois infractions ne pourront faire l'objet de poursuites, lorsqu'elles sont commises à l'encontre de particuliers, que si la personne qui se prétend offensée a porté plainte[145] [146].

Conformément à l'article 150 de la Constitution, les délits de presse, excepté ceux inspirés par le racisme ou la xénophobie, relèvent de la compétence de la Cour d'assises. Le délit de presse consiste en « *l'expression punissable d'une opinion dans un texte reproduit par voie d'imprimerie ou par un procédé similaire* »[147]. Traditionnellement, les éléments constitutifs du délit de presse sont les suivants :

- une infraction de droit commun (comme par exemple la calomnie, la diffamation ou l'injure) ;
- la manifestation d'une pensée ou d'une opinion ;
- la publicité
- au moyen d'un écrit reproduit[148] [149].

La Cour de cassation a, par deux arrêts du 6 mars 2012, considéré que des écrits diffusés par voie numérique pouvaient satisfaire à cette condition de « procédé similaire »[150]. Le délit de presse vise donc uniquement les écrits et non les contenus oraux ou audiovisuels[151] [152]. La Cour de cassation a confirmé sa jurisprudence, par un arrêt du 8 novembre 2016,

[143] A. DE NAUW et F. KUTY, *op. cit.*, pp. 624 à 626.
[144] Bruxelles (13e ch.), 4 avril 2007, *A&M*, 2009/1-2, p. 172.
[145] C. pén., art. 450, alinéa 1er.
[146] A. DE NAUW et F. KUTY, *op. cit.*, p. 630.
[147] H. BOSLY, E. DELHAISE, D. VANDERMEERSCH, N. COLETTE-BASECQZ, A. DE NAUW, P. MANDOUX et O. NEDERLANDT, « Chronique semestrielle de jurisprudence », *Rev. dr. pén.*, 2019/5, p. 571.
[148] Corr. Liège (div. Liège), 7 septembre 2018, *J.L.M.B.*, 2018/38, pp. 1819 et 1820, note Q. Pironnet.
[149] S. CARNEROLI, « Note sous Corr. Liège (16e ch.), 7 septembre 2018 », *A&M*, 2018-2019/1, p. 167.
[150] Cass. (2e ch.), 6 mars 2012, R.G. n° P.11.0855.N, *N.J.W*, 2012/9, n° 262, p. 341 ; Cass. (2e ch.), 6 mars 2012, R.G. n° P.11.1374.N, p. 2.
[151] C. cass. (2e ch.), 29 octobre 2013, R.G. n° P.13.1270.N, p. 3.
[152] Q. VAN ENIS, « La Cour de cassation admet que l'on puisse se rendre coupable d'un délit de presse sur l'internet. Le temps du "délit de presse 2.0" est-il (enfin) arrivé ? », *J.T.*, 2012/23, n° 6483, p. 506.

en considérant qu'une diffusion numérique constitue un « procédé similaire »[153]. Les cas d'application de délits de presse ne sont plus limités aux infractions traditionnelles de calomnie ou de dénonciation calomnieuse, mais se réfèrent désormais également à des faits pouvant être qualifiés de harcèlement[154].

Nous avons assisté à un revirement de jurisprudence, opéré par le tribunal correctionnel de Liège le 7 septembre 2018[155]. Dans le cas d'espèce, un entrepreneur voyant ses projets de construction rejetés de façon systématique a publié, au moyen de son profil public *Facebook*, des commentaires injurieux et harcelants à l'égard de l'échevine de l'urbanisme de la commune d'Awans. Cette dernière a décidé, au moyen d'une citation directe, d'agir pénalement[156]. Le prévenu a été déféré devant le tribunal correctionnel de Liège pour « *des faits d'injures, atteintes à l'honneur, harcèlement et menace d'attentat contre les personnes ou propriétés, à l'encontre d'une personnalité politique locale* »[157]. Malgré que les délits de presse relèvent de la compétence exclusive de la Cour d'assises, le tribunal s'est déclaré compétent, a refusé de qualifier les faits de délit de presse et a condamné l'auteur des faits à une peine de travail de 100 heures[158].

Le tribunal fonde sa décision sur le fait que l'interprétation donnée par la Cour de cassation ne prend pas en considération une réalité sociétale nouvelle. Les réseaux sociaux, comme *Facebook*, ne constituent pas des « forums » où des opinions peuvent être échangées, mais représentent une extension contemporaine de la parole. Cela « *illustre un véritable changement de paradigme quant à l'importance de l'écrit par rapport à l'oralité* »[159]. De plus, d'après le tribunal, cette jurisprudence n'est pas en conformité avec la pensée du constituant originel et entre en contradiction avec l'article 8 de la Convention européenne des droits de l'homme qui oblige les États à protéger de manière effective les citoyens en ce qui concerne leur droit à la vie privée et à l'honneur[160].

Quentin Pironnet préconise une conception fonctionnaliste du délit de presse qui tient compte de divers indices relatifs à l'auteur, à son intention, au contenu ainsi qu'à la forme par laquelle l'opinion est manifestée. C'est ainsi selon lui, que le juge pourra, en bénéficiant d'un certain pouvoir d'appréciation[161], qualifier, de délit de presse ou non, les faits lui étant

[153] Cass. (2e ch.), 8 novembre 2016, R.G. n° P.16.0958.N, p. 3.
[154] Corr. Flandre occidentale (div. Bruges), 19 avril 2016, *T.G.R.*, 2016, p. 300 ; Corr. Anvers (div. Anvers), 24 avril 2018, *N.J.W*, 2018, p. 649, note S. Royer.
[155] Corr. Liège (div. Liège), 7 septembre 2018, *J.L.M.B.*, 2018/38, p. 1817, note Q. Pironnet.
[156] S. CARNEROLI, *op. cit.*, p. 167.
[157] Q. PIRONNET, « Des insultes sur les réseaux sociaux ne relèvent pas du délit de presse », *J.L.M.B.*, 2018/38, p. 1825.
[158] S. CARNEROLI, *op. cit.*, p. 167.
[159] Q. PIRONNET, *op. cit.*, pp. 1826 et 1827.
[160] Corr. Liège (div. Liège), 7 septembre 2018, *J.L.M.B.*, 2018/38, p. 1822, note Q. Pironnet.
[161] Q. PIRONNET, *op. cit.*, p. 1829.

soumis, conformément à l'idée que le constituant originel avait de celui-ci[162]. Le tribunal avance qu'à l'origine, le délit de presse était seulement confiné aux journalistes et aux écrivains et visait donc un nombre restreint de personnes. Il argumente sa décision en constatant l'absence de « garde-fous » pour les simples particuliers. Ces « gardes-fous » peuvent être par exemple la déontologie ou l'encadrement professionnel étant aptes à prévenir ces délits. Concernant l'opinion, celle-ci doit, selon le tribunal, garder la forme d'une logique argumentative[163].

La conception fonctionnaliste citée précédemment consisterait en trois faisceaux d'indices afin d'aider le juge à qualifier les faits de délit de presse. Tout d'abord, l'expression doit émaner d'un journaliste ou « pamphlétaire ». Un « pamphlétaire » se définit comme un agitateur d'idées et doit être reconnu comme tel dans une certaine mesure. Ensuite, il reviendra au juge de prendre en compte l'intentionnalité et la forme de l'opinion diffusée en gardant à l'esprit les notions de « propagande », « logique argumentative », « pamphlets », etc. C'est ainsi que le juge pourra traiter distinctement une attaque ad hominem lorsqu'elle celle-ci prend place, à l'encontre d'un ministre, dans le cadre d'une publication par un collectif sur une page *Facebook* totalement publique et le harcèlement systématique sur *Instagram* par un adolescent à l'égard d'un autre élève. Enfin, le juge doit avoir égard aux destinataires de l'opinion émise en insistant sur la nécessité d'une large publicité de celle-ci afin de maintenir l'idée d'origine qui est celle de protéger la « communication de masse ». Par exemple, une campagne consistant en la diffusion de vidéos, d'affiches et de publications sur *Facebook*, lancée par des influenceurs dans le but de faire abroger la « taxe tampon » pourra être qualifiée de délit de presse. Par contre, le tribunal correctionnel resterait compétent concernant un ancien compagnon qui distribue, dans la société où travaille son ex-compagne, des feuillets l'insultant[164].

D'après Quentin Pironnet, ce jugement est bienvenu et audacieux et permet ainsi d'éviter l'impunité de fait de l'auteur présumé des infractions[165]. En effet, pour Marc Isgour, la compétence exclusive de la Cour d'assises concernant la diffusion punissable d'une opinion sur Internet « *est cependant très dommageable pour les victimes de ces atteintes qui ne pourront plus envisager qu'une action civile en dommages et intérêts étant donné l'impunité de fait que connaissent les délits de presse* »[166]. Il y a lieu de préciser que dans l'esprit du constituant originel, au vu du nombre restreint de bénéficiaires de l'ancien article

[162] *Ibid*., p. 1828.
[163] Corr. Liège (div. Liège), 7 septembre 2018, *J.L.M.B*., 2018/38, p. 1821, note Q. Pironnet.
[164] Q. PIRONNET, *op. cit*., pp. 1829 et 1830.
[165] *Ibid*., p. 1825.
[166] M. ISGOUR, « La protection juridique de l'e-réputation des personnes physiques et morales », *L'élément moral en droit. Une vision transversale*, sous la direction de F. Lambinet, Limal, Anthemis, 2014, p. 103.

98 de la Constitution, une infraction de presse, relevant dès lors de la compétence de la Cour d'assises, ne rimait pas avec une impunité de fait[167].

Le jugement du tribunal correctionnel de Liège a été confirmé par la Cour d'appel de Liège le 28 mai 2019. La cour a considéré que dans le cas d'espèce, il ne s'agissait pas de l'expression d'une opinion, mais uniquement d'une profération d'insultes et que dès lors, les faits ne pouvaient être qualifiés de délit de presse. La cour a alourdi la sanction infligée par le tribunal correctionnel de Liège. La peine de travail initialement prévue a été muée en un emprisonnement de dix mois[168].

Chapitre 3. L'irresponsabilité du cyber-harceleur mineur

Comme nous l'avons vu précédemment, le taux le plus haut de victimisation de harcèlements et d'intimidations en ligne touche la tranche d'âge 15-24 ans[169]. Le 14 avril 2016, le journal *La Libre* a publié des statistiques alarmantes. D'après une étude réalisée par *Ipsos* en 2015, les jeunes âgés entre 13 et 19 ans passent en moyenne 13h30 par semaine sur Internet. Alors que 27% des 2500 jeunes du secondaire interrogés affirment avoir déjà fait l'objet d'insultes sur le Net, 25% avouent avoir déjà été auteurs d'insultes en ligne[170].

Ces statistiques permettent de faire le constat suivant : le cyber-harcèlement est un phénomène qui touche un grand nombre de jeunes, aussi bien en tant qu'auteurs que victimes.

Lorsque les jeunes ne disposent pas de la majorité pénale au moment de la commission des faits, c'est-à-dire lorsqu'ils sont âgés de moins de 18 ans accomplis, ils bénéficient d'une présomption d'irresponsabilité pénale instaurée par le législateur de par leur absence de discernement. Dès lors, le tribunal de la jeunesse est compétent[171] [172]. Le tribunal de la jeunesse peut ordonner, à l'égard du mineur, des mesures de garde, de préservation et

[167] Q. PIRONNET, *op. cit.*, p. 1830.
[168] L. WAUTERS, « "Injurier n'est pas exprimer une opinion" : prison ferme pour des propos sur Facebook », 28 mai 2019, *Le Soir+*, disponible sur https://plus.lesoir.be/227594/article/2019-05-28/injurier-nest-pas-exprimer-une-opinion-prison-ferme-pour-des-propos-sur-facebook (31 juillet 2019).
[169] Voy., *supra*, Partie 1, Chapitre 3, p. 7.
[170] A. HOVINE, « Cyber-harcèlement : Un quart des jeunes ont déjà été insultés sur internet », 14 avril 2016, *La Libre*, disponible sur https://www.lalibre.be/belgique/cyber-harcelement-un-quart-des-jeunes-ont-deja-ete-insultes-sur-internet-570e717335702a22d65948eb (28 juillet 2019).
[171] Art. 36, 4°, de la loi du 8 avril 1965 relative à la protection de la jeunesse, à la prise en charge des mineurs ayant commis un fait qualifié infraction et à la réparation du dommage causé par ce fait, *M.B.*, 15 avril 1965, (ci-après abrégée « loi du 8 avril 1965 »).
[172] F. KUTY, « La minorité pénale », *Principes généraux du droit pénal belge*, Bruxelles, Larcier, 2010, pp. 387 et 388 ; N. COLETTE-BASECQZ, « La responsabilité pénale liée au phénomène du cyberharcèlement et à ses différentes formes d'expression », *op. cit.,* p. 39.

d'éducation en prenant en compte différents facteurs[173]. Le tribunal dispose donc de la possibilité d'imposer, le cas échéant cumulativement, au mineur une multitude de mesures de protection de la jeunesse allant de la réprimande au placement dans une section fermée d'un service pédopsychiatrique[174] [175]. Il peut également, si plusieurs conditions sont remplies, « *faire une offre restauratrice de médiation et de concertation restauratrice en groupe* »[176].

Si lorsqu'au moment des faits, le mineur est âgé de 16 ans ou plus et que le tribunal de la jeunesse n'estime pas adéquat d'imposer une mesure de garde, de préservation ou d'éducation, une procédure de dessaisissement peut être décidée par le tribunal. Dès lors, l'affaire est renvoyée au ministère public aux fins de poursuite. En cas de délit ou de crime correctionnalisable, les poursuites peuvent être intentées devant une chambre spécifique au sein du tribunal de la jeunesse appliquant le droit pénal commun et la procédure pénale commune. En cas de crime non correctionnalisable, le ministère public peut poursuivre le mineur devant une Cour d'assises composée d'au moins deux magistrats[177]. Ces magistrats doivent avoir suivi une formation spécialisée continue organisée par l'Institut de formation judiciaire[178]. Le tribunal ne peut se dessaisir que si le mineur a déjà fait l'objet d'une ou plusieurs mesures de protection de la jeunesse ou d'une offre restauratrice et/ou si le fait dont il est question est visé par les articles cités par l'article 57*bis*, 1er, alinéa 1er, deuxième tiret, de la loi du 8 avril 1965.

[173] Art. 37, § 1er, alinéas 1er et 2, de la loi du 8 avril 1965.
[174] Art. 37, § 2, alinéa 1er, de la loi du 8 avril 1965.
[175] N. COLETTE-BASECQZ, « La responsabilité pénale liée au phénomène du cyberharcèlement et à ses différentes formes d'expression », *op. cit.*, p. 39.
[176] Art. 37*bis*, § 1er, alinéa 1er, de la loi du 8 avril 1965.
[177] Art. 57*bis*, § 1er, alinéa 1er, de la loi du 8 avril 1965.
[178] C. jud., art. 119, § 2, et 259*sexies*, § 1er, 1°, alinéa 3 et 2°, alinéa 2.

Partie 3. La preuve numérique et les moyens juridiques mis en place pour la collecte de celle-ci

Chapitre 1. La preuve numérique

Comme nous l'avons vu précédemment, plusieurs instruments juridiques protègent le secret des communications[179]. Il convient dès lors de s'interroger sur l'admissibilité d'une telle preuve. Depuis l'arrêt de principe en matière pénale de la Cour de cassation du 14 octobre 2003, communément connu sous le nom arrêt « Antigone », le juge n'est plus dans l'obligation d'écarter des débats une preuve irrégulièrement recueillie[180].

Dans cet arrêt, la Cour de cassation dégage trois hypothèses dans lesquelles le juge ne peut prendre en considération, de manière directe ou indirecte, la preuve irrégulièrement obtenue :

> « - *Soit lorsque le respect de certaines conditions de forme est prescrit à peine de nullité ;*
> - *Soit lorsque l'irrégularité commise a entaché la fiabilité de la preuve ;*
> - *Soit lorsque l'usage de la preuve est contraire au droit à un procès équitable ;* »[181].

Le législateur a, par la loi du 24 octobre 2013[182], inséré le principe édicté par la jurisprudence Antigone dans l'article 32 du titre préliminaire du Code d'instruction criminelle.

Chapitre 2. Les méthodes d'enquête

En principe, la seule personne pouvant poser un acte de contrainte susceptible de porter atteinte aux droits et libertés individuelles est le juge d'instruction. Alors que celui-ci a pour compétence d'instruire à charge, et à décharge, de manière indépendante et impartiale, le procureur du Roi, quant à lui, joue un rôle de poursuite. Mais, cette

[179] Voy., *supra*, Introduction, p. 2.
[180] G. MASSART, « Régularité de la preuve: un cadre légal pour la jurisprudence Antigone », 16 décembre 2013, *Elegis*, disponible sur http://www.elegis.be/fr/nouvelle/regularite-de-la-preuve-un-cadre-legal-pour-la-jurisprudence-antigone (27 mars 2019).
[181] Cass. (2e ch.), 14 octobre 2003, R.G. n° P.03.0762.N, p. 2.
[182] Loi du 24 octobre 2013 modifiant le titre préliminaire du Code de procédure pénale en ce qui concerne les nullités, *M.B.*, 12 novembre 2013.

répartition de rôles a fait l'objet d'une grande modification par la loi du 25 décembre 2016 afin de s'aligner aux besoins des enquêteurs dans un contexte numérique. Cette loi clarifie certaines controverses et offre de nouvelles méthodes d'enquête[183] [184].

Section 1. La préservation de données

La préservation de données est une des nouvelles méthodes d'enquête insérée dans le Code d'instruction criminelle par la loi du 25 décembre 2016. L'article 39*ter* du Code d'instruction criminelle permet à tout officier de police judiciaire d'ordonner, par décision écrite motivée contenant plusieurs mentions ou, verbalement en cas d'urgence, la conservation de données possédées ou contrôlées par une ou plusieurs personnes physiques ou morales. Pour ce faire, il doit exister des raisons de penser que la perte ou la modification de données stockées, traitées ou transmises au moyen d'un système informatique est particulièrement susceptible de se produire. La durée de conservation maximale est de nonante jours, sous réserve d'une prolongation par écrit[185]. Ce délai est prévu afin que d'autres procédures demandant l'accomplissement de formalités complémentaires soient mises en place par les autorités[186]. La disparition, destruction, modification des données conservées par toute personne, ainsi que le refus de coopérer sont punis d'un emprisonnement allant de six mois à un an et/ou d'une amende de vingt-six euros à vingt mille euros[187].

En vertu de l'article 39*quater,* paragraphe 1er, du Code d'instruction criminelle, le procureur du Roi a la possibilité, par l'intermédiaire du service de police désigné par le Roi, de demander à une autorité étrangère compétente la conservation de données se trouvant sur le territoire de celle-ci et nécessitant l'émission d'une demande d'entraide judiciaire[188]. Corrélativement et de manière similaire, une autorité compétente d'un État peut demander au service de police désigné par le Roi la conservation de données se trouvant sur le territoire belge, à condition qu'une telle possibilité soit prévue dans un instrument de droit international liant la Belgique et cet autre État[189].

[183] 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, (ci-après abrégée « loi du 25 décembre 2016 »).
[184] C. FORGET, « 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 et 26.
[185] C.i.cr., art. 39*ter,* § 1er.
[186] C. FORGET, « Les nouvelles méthodes d'enquête dans un contexte informatique : vers un encadrement (plus) strict », *op. cit.*, p. 27.
[187] C.i.cr., art. 39t*er,* § 3, alinéa 2.
[188] C.i.cr., art. 39*quater,* § 1er.
[189] C.i.cr., art. 39*quater,* § 2.

Section 2. La saisie de données informatiques, la recherche et l'extension de la recherche dans un système informatique, sans but secret

Il y a lieu d'analyser qui est compétent en matière de saisie de données informatiques, de recherche et d'extension de la recherche dans un système informatique. Auparavant, le régime en vigueur distinguait la saisie de la recherche et de l'extension de la recherche. Alors que le procureur du Roi était compétent concernant la première méthode, le juge d'instruction l'était pour les deux dernières[190]. Cette procédure soulevait de nombreuses controverses, car le Code d'instruction criminelle ne précisait pas si l'exploitation d'un système informatique pouvait être réalisée par les enquêteurs dans le cas où le juge d'instruction n'avait pas rendu une ordonnance à cet égard[191]. Par sa jurisprudence de 2015, ensuite entérinée dans la loi du 25 décembre 2016, la Cour de cassation a supprimé la nécessité de distinguer la saisie de la recherche. Selon la cour, la mesure consistant à exploiter la mémoire d'un téléphone portable, en ce compris les messages stockés sous forme d'un SMS découle de la saisie. Cet acte d'enquête peut être réalisé lors d'une information sans que d'autres formalités, excepté celles requises pour cet acte, ne doivent être remplies[192].

1. La recherche et son extension

Tout d'abord, il est nécessaire de s'interroger sur la signification et la distinction entre « secret » et « non secret ». D'après les travaux parlementaires, afin de distinguer ces deux notions, il est nécessaire, en premier lieu, d'identifier si l'intention des enquêteurs est « *de prendre connaissance des communications ou des données à l'insu des acteurs de ces communications ou à l'insu du propriétaire, du détenteur ou de l'utilisateur du système informatique* »[193]. En second lieu, le procureur du Roi ou le juge d'instruction est dans l'obligation de procéder à une notification de la recherche ou de son extension à la personne responsable du système informatique, et ce dans les plus brefs délais[194]. De cette obligation découle le caractère non secret de la recherche ou son extension[195]. Il existe une exception à cette obligation de notification dans le cas où l'identité ou l'adresse du responsable du système informatique ne peut être trouvée de manière raisonnable[196]. Les

[190] C.i.cr., art. 39*bis* et 88*ter.*
[191] C. FORGET, « Les nouvelles méthodes d'enquête dans un contexte informatique : vers un encadrement (plus) strict », *op. cit.*, p. 29.
[192] Cass. (2e ch.), 11 février 2015, R.G. n° P.14.1739.F, p. 3.
[193] Projet de loi relatif à l'amélioration des méthodes particulières de recherche et de certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications, Exposé des motifs, *Doc. parl.*, Chambre, 2015-2016, n° 54-1966/1, p. 54, 8 juillet 2016.
[194] C.i.cr., art. 39*bis,* § 7.
[195] C. FORGET, « Les nouvelles méthodes d'enquête dans un contexte informatique : vers un encadrement (plus) strict », *op. cit.*, p. 30.
[196] C.i.cr., art. 39*bis,* § 7.

travaux préparatoires ne précisent pas ce qu'il y a lieu d'entendre par « raisonnablement », ce qui permet aux enquêteurs de disposer d'une certaine marge d'appréciation[197]. Ce responsable est l'individu contrôlant réellement ou juridiquement le système[198]. Par conséquent, la personne qui voit ses données exploitées n'est pas forcément la personne responsable ayant le contrôle[199]. Ainsi, lorsqu'un ordinateur placé dans un cybercafé fait l'objet d'une exploitation par les autorités, tant le propriétaire que l'utilisateur du système peuvent se voir notifier la recherche ou son extension[200].

La recherche ou son extension sans but secret devront respecter les conditions prévues à l'article 39*bis* du Code d'instruction criminelle. Si, au contraire et comme nous le verrons par la suite, la recherche ou son extension sont secrètes, les conditions de l'article 90*ter* du Code d'instruction criminelle devront être observées. Malgré que le niveau d'ingérence soit similaire, il existe de grandes différences procédurales, et dès, lors de grandes disparités concernant les garanties offertes. Le cadre juridique est distinctement plus souple dans le cadre d'une recherche ou extension sans but secret[201].

Il y a lieu de distinguer trois hypothèses qui constituent, de manière croissante, une ingérence dans la vie privée de celui qui en fait l'objet[202]. Premièrement, la recherche à l'occasion d'une saisie éventuelle du support. Deuxièmement, l'extension de la recherche lors d'une saisie éventuelle de support. Troisièmement, la recherche et l'extension de la recherche indépendamment de la saisie éventuelle du support.

1.1. La recherche à l'occasion d'une saisie éventuelle de support

Dans la première hypothèse, il est permis à tout officier de police judiciaire d'effectuer une recherche. Cela signifie que celui-ci peut lire, inspecter ou examiner des données[203] dans un système informatique. La recherche ne peut être effectuée qu'après que le support ait été saisi et à condition que l'appareil ne soit pas verrouillé ou que l'enquêteur dispose du

[197] C. FORGET, « Les nouvelles méthodes d'enquête dans un contexte informatique : vers un encadrement (plus) strict », *op. cit.*, p. 30.
[198] Projet de loi relatif à l'amélioration des méthodes particulières de recherche et de certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications, Exposé des motifs, *Doc. parl.*, Chambre, 2015-2016, n° 54-1966/1, p. 21, 8 juillet 2016.
[199] V. FRANSSEN et S. TOSZA, « Vers plus de droits pour le justiciable sur internet ? Un nouveau cadre légal pour lutter contre la criminalité dans la société de l'information », *Les droits des justiciables face à la justice pénale*, Limal, Anthemis, 2017, p. 223.
[200] C. FORGET, « Les nouvelles méthodes d'enquête dans un contexte informatique : vers un encadrement (plus) strict », *op. cit.*, p. 30.
[201] *Ibid.*, pp. 30 et 31.
[202] O. MICHIELS et G. FALQUE, « Les actes d'enquête », *Principes de procédure pénale*, Bruxelles, Larcier, 2019, p. 193.
[203] CONSEIL DE L'EUROPE, « Rapport explicatif de la Convention sur la cybercriminalité », Budapest, 23 novembre 2001, § 191, p. 38, disponible sur https://rm.coe.int/16800ccea4 (25 juin 2019).

code d'accès[204] [205]. Par exemple, un ordinateur, un smartphone, un GPS ou une clé USB pourront faire l'objet d'une recherche[206]. Dans le cas où le support pourrait être saisi, mais pour lequel le procureur du Roi n'a pas jugé opportun de saisir, l'officier doit, préalablement à la recherche, disposer d'une autorisation du procureur du Roi[207]. L'officier doit également obtenir une autorisation du procureur du Roi dans le cas où, pour accéder aux données, il y a lieu de supprimer une protection, décrypter ou décoder les données[208] [209].

Dans cette première hypothèse, la recherche doit être uniquement limitée aux données sauvegardées sur l'appareil. Par conséquent, durant l'enquête, toute liaison externe doit être coupée[210]. Cela peut se faire, par exemple, en activant le mode avion du téléphone. De la sorte, les enquêteurs ne disposent pas d'un accès direct aux informations circulant via des services tels que *WhatsApp*, *Viber*, *Hotmail*, *Gmail* ou *Facebook*, excepté si celles-ci sont sauvegardées et accessibles « hors connexion »[211].

La recherche est donc dépendante de la saisie. Cela parait difficilement compatible avec la Recommandation n° R(95)13 du Conseil de l'Europe[212] et la Convention de Budapest[213]. En vertu de ces dispositions, la procédure applicable en cas d'intrusion dans un système informatique dans le but de saisir des données doit être réalisée dans des conditions similaires à celles prévues « *dans le cadre des pouvoirs traditionnels de perquisition et de saisie* ». La loi du 25 décembre 2016 aligne donc la procédure concernant la recherche à celle prévue en cas de saisie et non à celle relative à la perquisition. Ainsi, malgré une grande immixtion dans le droit au respect de la vie privée du justiciable, celui-ci bénéficie de peu de garanties[214]. Selon la Cour européenne des droits de l'homme, une autorisation est, à l'instar d'une mesure de perquisition et sauf exception, nécessaire préalablement à la recherche[215]. Cette autorisation donne la possibilité d'être certain de l'existence de soupçons raisonnables vis-à-vis de l'intéressé, et ce, avant que les enquêteurs

[204] C.i.cr., art. 39*bis,* § 2, alinéa 1er.
[205] C. FORGET, « Les nouvelles méthodes d'enquête dans un contexte informatique : vers un encadrement (plus) strict », *op. cit.*, p. 31.
[206] O. MICHIELS et G. FALQUE, *op. cit.*, p. 193.
[207] *Ibid.*, p. 194.
[208] C.i.cr., art. 39*bis*, § 5, alinéa 1er.
[209] C.C., 6 décembre 2018, n° 174/2018, B.3.3.
[210] C.i.cr., art. 39*bis,* § 2, alinéas 2 et 3.
[211] Projet de loi relatif à l'amélioration des méthodes particulières de recherche et de certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications, Exposé des motifs, *Doc. parl.*, Chambre, 2015-2016, n° 54-1966/1, pp. 16 et 17, 8 juillet 2016.
[212] Recommandation du Comité des ministres du 11 septembre 1995 aux États membres relative aux problèmes de procédure pénale liés à la technologie de l'information (R(95)13), § 2, p. 2.
[213] CONSEIL DE L'EUROPE, « Rapport explicatif de la Convention sur la cybercriminalité », Budapest, 23 novembre 2001, § 191, p. 38, disponible sur https://rm.coe.int/16800ccea4 (25 juin 2019).
[214] C. FORGET, « Les nouvelles méthodes d'enquête dans un contexte informatique : vers un encadrement (plus) strict », *op. cit.*, p. 31.
[215] Cour eur. D.H., arrêt Trabajo Rueda c. Espagne, 30 mai 2017, req. n° 32600/12, § 35.

n'interviennent dans le système[216]. Ceci permet de ne pas procéder arbitrairement et empêcher une « *saisie* » « *massive et indifférenciée* »[217] [218]. Celle-ci, également dénommée *fishing expeditions,* consiste à fouiller afin de découvrir la preuve d'une infraction et partant, constitue une violation du droit au respect de la vie privée[219] [220].

1.2. L'extension de la recherche lors d'une saisie éventuelle de support

L'extension de la recherche permet tout d'abord aux enquêteurs d'accéder à l'entièreté des données ayant été enregistrées ou sauvegardées sur l'appareil, ce qui représente le point de départ de la recherche. De plus, elle donne accès à l'ensemble des documents stockés sur les systèmes informatiques pouvant être atteint par connexion. Enfin, elle permet d'avoir accès à l'intégralité des communications entre l'utilisateur et des tiers, y compris les nouveaux messages réceptionnés ou en cours de réception dont il n'a pas encore connaissance[221].

Avant l'arrêt de la Cour constitutionnelle du 6 décembre 2018, l'extension de la recherche, vers d'autres systèmes ou parties de ceux-ci, entamée à partir d'une saisie éventuelle de support était une compétence appartenant au procureur du Roi[222].

Le procureur du Roi était compétent à condition qu'aucun mot de passe ne doive être introduit par les enquêteurs. Prenons un exemple développé dans les travaux préparatoires. Généralement, afin d'accéder au compte *Facebook* du smartphone saisi, au moyen de l'application dédiée, aucun mot de passe ne doit être introduit car celui-ci a été « retenu ». Dans une telle situation, le procureur du Roi pouvait ordonner la prise de connaissance des données *Facebook* étant déjà dans le smartphone lors de la saisie. De plus, il pouvait enjoindre de mettre à jour les données *Facebook* et ainsi prendre connaissance des données n'étant peut-être pas encore physiquement présentes dans le smartphone au moment de sa saisie.

Au contraire, dans le cas où un mot de passe devait être introduit, et ce, peu importe qu'il soit identique à celui requis pour accéder au système d'exploitation, il revenait au juge

[216] Cour eur. D.H., arrêt Vinci construction et GMT Génie Civil et services c. France, 2 avril 2014, req. n° 63629/10, §§ 78 et 79 et C. FORGET, « Les nouvelles méthodes d'enquête dans un contexte informatique : vers un encadrement (plus) strict », *op. cit*., p. 32.
[217] Cour eur. D.H., arrêt Maschino c. France, 16 octobre 2008, req. n° 10447/03, § 34.
[218] C. FORGET, « Les nouvelles méthodes d'enquête dans un contexte informatique : vers un encadrement (plus) strict », *op. cit*., p. 32.
[219] Cour eur. D.H., arrêt Vinci construction et GMT Génie Civil et services c. France, 2 avril 2014, req. n° 63629/10, §§ 78 et 79.
[220] C. FORGET, « Les nouvelles méthodes d'enquête dans un contexte informatique : vers un encadrement (plus) strict », *op. cit*., p. 32.
[221] C.C., 6 décembre 2018, n° 174/2018, B.11.2.
[222] C.i.cr., art. 39*bis,* § 3, alinéa 1er.

d'instruction de donner son autorisation[223]. Par conséquent, l'intervention du juge d'instruction et ainsi l'existence d'une garantie supplémentaire étaient liées à l'unique possibilité qu'un mot de passe soit retenu par un système informatique.

La Cour constitutionnelle a, par son arrêt du 6 décembre 2018, annulé le paragraphe 3 de l'article 39*bis* du Code d'instruction criminelle, inséré par l'article 2 de la loi du 25 décembre 2016. De plus, la cour a considéré qu'il était nécessaire d'annuler l'article 13 de la loi du 25 décembre 2016 abrogeant l'article 88*ter* du Code d'instruction criminelle, en ce qu'il est lié de manière indissociable à la disposition attaquée. Cet arrêt opère donc le rétablissement de l'article 88*ter* du Code d'instruction criminelle. L'article 11 de la loi du 5 mai 2019[224] a réintroduit l'article 88*ter*[225], quelque peu modifié.

La cour fonde sa décision sur le fait que les réseaux accessibles à partir des systèmes informatiques se sont développés de manière remarquable et sont fortement utilisés par la plupart des citoyens. Les individus y stockent des documents et données, parfois très intimes, relevant de leur vie privée. Par conséquent, une mesure d'investigation donnant accès à la totalité des données et communications présentes sur les réseaux connectés à un système informatique appartenant à une personne cause une ingérence dans son droit au respect de la vie privée. Cette ingérence est comparable à celles constituées par une mesure de perquisition dans un domicile ou lieu privé (articles 87 et 88 du Code d'instruction criminelle) de même que par une interception des communications électroniques (article 90*ter* du Code d'instruction criminelle) ou courrier postal (article 88*sexies* du Code d'instruction criminelle).

Les droits de la défense sont moins garantis lors d'une information qu'au cours d'une instruction, car l'information présente un caractère secret et non contradictoire. Le législateur a justifié la différence de traitement par le caractère non secret de l'investigation. Le paragraphe 7 de l'article 39*bis* contient une obligation d'information. La recherche ou son extension doivent être notifiées au responsable du système informatique faisant l'objet de l'investigation, dans les plus brefs délais et excepté si son identité ou son adresse ne peuvent être raisonnablement trouvées. Mais cette obligation d'information comporte aussi une grande ingérence dans le droit au respect de la vie privée de l'intéressé puisque le fait qu'il soit informé n'implique pas qu'il y ait consenti.

[223] C.i.cr., art. 39*bis,* § 5, alinéa 2 ; Projet de loi relatif à l'amélioration des méthodes particulières de recherche et de certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications, Exposé des motifs, *Doc. parl.*, Chambre, 2015-2016, n° 54-1966/1, p. 20, 8 juillet 2016.
[224] Art. 11 de la loi du 5 mai 2019 portant des dispositions diverses en matière pénale et en matière de cultes, et modifiant la loi du 28 mai 2002 relative à l'euthanasie et le Code pénal social, *M.B.*, 24 mai 2019, (ci-après abrégée « loi du 5 mai 2019 »).
[225] Voy., art. 8 de la loi du 28 novembre 2000 relative à la criminalité informatique, *M.B.*, 3 février 2001, (ci-après abrégée « loi du 28 novembre 2000 »).

En vertu de l'article 28*bis*, paragraphe 3, alinéa 1er, du Code d'instruction criminelle, les mesures d'investigation réalisées durant l'enquête pénale portant atteinte aux libertés et aux droits individuels ne peuvent être, en principe, accomplies que dans le cadre d'une instruction. C'est pourquoi l'extension de la recherche ne peut être autorisée que si elle répond aux conditions requises en ce qui concerne la perquisition et l'interception des communications électroniques ou du courrier postal, mesures requérant l'intervention d'un juge d'instruction. En effet, l'intervention préalable du juge d'instruction, étant indépendant et impartial, garantit que l'ingérence occasionnée dans le droit au respect de la vie privée soit proportionnée au prescrit de l'article 22 de la Constitution et de l'article 8 de la Convention européenne des droits de l'homme[226].

L'article 11 de la loi du 5 mai 2019 a réintroduit l'article 88*ter*[227], quelque peu modifié, que nous énoncerons ci-dessous. Conformément à cet article :

« *Le juge d'instruction peut étendre la recherche dans un système informatique ou une partie de celui-ci, entamée sur la base de l'article 39bis, vers un système informatique ou une partie de celui-ci qui se trouve dans un autre lieu que celui où la recherche est effectuée :*

- si cette extension est nécessaire pour la manifestation de la vérité à l'égard de l'infraction qui fait l'objet de la recherche; et

- si d'autres mesures étaient disproportionnées, ou s'il existe un risque que, sans cette extension, des éléments de preuve soient perdus.

L'extension de la recherche dans un système informatique ne peut pas excéder les systèmes informatiques ou les parties de tels systèmes auxquels les personnes autorisées à utiliser le système informatique qui fait l'objet de la mesure ont spécifiquement accès. En ce qui concerne les données recueillies par l'extension de la recherche dans un système informatique, qui sont utiles pour les mêmes finalités que celles prévues pour la saisie, les règles prévues à l'article 39bis, § 6 s'appliquent.

Lorsqu'il s'avère que ces données ne se trouvent pas sur le territoire du Royaume, elles peuvent seulement être copiées. Dans ce cas, le juge d'instruction communique sans délai cette information au Service public fédéral Justice, qui en informe les autorités compétentes de l'état concerné, si celui-ci peut raisonnablement être déterminé.
[...] ».

1.3. La recherche et l'extension de la recherche indépendamment de la saisie éventuelle du support

Le juge d'instruction est exclusivement compétent pour autoriser toute recherche dans un système informatique autre que celle visée par le paragraphe 2 de l'article 39*bis* du Code

[226] C.C., 6 décembre 2018, n° 174/2018, B.14.4 à B.15.4.
[227] Voy., art. 8 de la loi du 28 novembre 2000.

d'instruction criminelle. Cette disposition concerne la recherche dans un système informatique à distance. Autrement dit, la recherche s'effectuera sur base des ordinateurs des enquêteurs[228]. Par exemple, le juge d'instruction est compétent pour effectuer une recherche dans un compte Gmail connecté à un appareil n'ayant pas été saisi[229].

La disposition en question ne règle pas expressément le cas de l'extension de la recherche, mais celle-ci peut se déduire du dernier alinéa du paragraphe 4 de l'article 39*bis* du Code d'instruction criminelle prévoyant la possibilité d'autoriser oralement une extension de la recherche en cas d'urgence. Selon les travaux parlementaires, dans le cadre d'une extension de la recherche visée par le paragraphe 4, les conditions d'application du paragraphe 3, désormais contenues à l'article 88*ter*, s'appliquent naturellement[230]. Par conséquent, l'extension de la recherche doit se limiter aux parties auxquelles les personnes ayant reçu l'autorisation d'utiliser le système informatique ont accès de manière spécifique. De plus, tant pour la recherche que pour l'extension de la recherche, deux conditions doivent être remplies. D'une part, les mesures doivent être nécessaires pour la manifestation de la vérité. D'autre part, il faut que le critère de proportionnalité soit rempli ou qu'il existe un risque de perte d'éléments de preuve[231].

2. *La saisie*

L'exploitation de données informatiques est une mesure qui découle de la saisie. Par conséquent, le législateur n'a pas expressément distingué la recherche de la saisie[232]. Lorsqu'il n'est pas souhaitable de saisir le support, la copie des données peut être ordonnée. La copie peut avoir lieu sur un support qui appartient aux autorités, ou, sur des supports disponibles en cas d'urgence ou pour des raisons techniques[233].

Lorsqu'il n'est pas possible de copier les données en raison de leur volume ou pour des raisons techniques, le procureur du Roi dispose de la faculté d'empêcher l'accès aux données en assurant la conservation de leur intégrité[234]. L'accès aux données peut être interdit ou celles-ci peuvent être retirées par le procureur du Roi, après les avoir copiées. Pour ce faire, il est nécessaire que les données constituent l'objet de l'infraction ou qu'elles

[228] O. MICHIELS et G. FALQUE, *op. cit*., p. 195.
[229] Projet de loi relatif à l'amélioration des méthodes particulières de recherche et de certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications, Exposé des motifs, *Doc. parl.*, Chambre, 2015-2016, n° 54-1966/1, p. 21, 8 juillet 2016.
[230] Projet de loi relatif à l'amélioration des méthodes particulières de recherche et de certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications, Exposé des motifs, *Doc. parl.*, Chambre, 2015-2016, n° 54-1966/1, p. 21, 8 juillet 2016.
[231] C.i.cr., art. 39*bis,* §§ 3, alinéa 1er, et 4, alinéa 1er.
[232] Cass. (2e ch.), 11 février 2015, R.G. n° P.14.1739.F, p. 3.
[233] C.i.cr., art. 39*bis,* § 6, alinéa 1er.
[234] C.i.cr., art. 39*bis,* § 6, alinéa 3.

aient été créées par l'infraction. De plus, ces données doivent être contraires à l'ordre public ou aux bonnes mœurs ou présenter un danger en ce qui concerne l'intégrité des systèmes informatiques ou des données stockées, traitées ou transmises via de tels systèmes[235].

Tel était également le régime applicable avant l'adoption de la loi du 25 décembre 2016. Néanmoins, cette même loi a introduit une nouveauté et il est désormais permis au procureur du Roi d'utiliser ultérieurement les données saisies, ou une partie de celles-ci, lorsque l'exercice des poursuites n'est pas mis en danger par cet usage. Les seules données pour lesquelles l'utilisation ultérieure est interdite sont les données, citées précédemment, pouvant être rendues inaccessibles ou retirées[236] [237].

Le responsable est en droit de recevoir un résumé des données copiées, rendues inaccessibles ou retirées[238]. Dès lors, ce dernier peut exercer le recours prévu à l'article 28*sexies* du Code d'instruction criminelle. En vertu de cette disposition, une fois que le responsable démontre « être lésé », il peut demander la levée d'un acte d'information concernant ses biens. Selon la Cour européenne des droits de l'homme, afin qu'un recours soit effectif, l'intéressé doit pouvoir s'adresser à un juge afin de contester la régularité de la mesure et partant, que les documents saisis lui soient restitués ou effacés[239]. C'est uniquement en analysant la pratique que nous pourrons constater si l'article 39*bis*, paragraphe 7, combiné à l'article 28*sexies* du Code d'instruction criminelle offrent la possibilité d'exercer un recours effectif, au sens de la jurisprudence précédemment citée[240].

3. Comment déverrouiller un système informatique ?

Le procureur du Roi ou le juge d'instruction peut user de fausses clés, et ce, sans le consentement du propriétaire, de son ayant droit ou de l'utilisateur[241]. Une fausse clé se définit comme étant « *tout moyen utilisé dans le but de contourner ou de craquer la sécurité d'un système informatique ou d'une partie de celui-ci afin d'obtenir l'accès – sous forme lisible – aux données contenues dans ce système* ». L'utilisation de fausses clés est absolument nécessaire lorsque le suspect refuse de communiquer son mot de passe ou

[235] C.i.cr., art. 39*bis,* § 6, alinéa 4.
[236] C.i.cr., art. 39*bis,* § 6, alinéa 5.
[237] C. FORGET, « Les nouvelles méthodes d'enquête dans un contexte informatique : vers un encadrement (plus) strict », *op. cit.*, pp. 34 et 35.
[238] C.i.cr., art. 39*bis,* § 7.
[239] Cour eur. D.H., arrêt Vinci construction et GMT Génie Civil et services c. France, 2 avril 2014, req. n° 63629/10, § 78.
[240] C. FORGET, « Les nouvelles méthodes d'enquête dans un contexte informatique : vers un encadrement (plus) strict », *op. cit.*, p. 36.
[241] C.i.cr., art. 39*bis,* § 5.

lorsque l'appareil fait l'objet d'une saisie régulière, mais que l'identité de son propriétaire est inconnue. Afin de ne pas prendre le risque que des données soient effacées ou que des éléments de preuves disparaissent, le suspect ne doit pas avoir la possibilité, au préalable, d'introduire lui-même le code d'accès[242]. Lorsque cela est spécifiquement nécessaire pour l'application de l'article 88*ter* du Code d'instruction criminelle, seul le juge d'instruction est compétent pour supprimer temporairement toute protection des systèmes informatiques concernés, notamment au moyen de fausses clés, ou installer des dispositifs techniques[243].

Section 3. L'interception, la prise de connaissance, l'exploration et l'enregistrement, dans un but secret, de communications non accessibles au public ou des données d'un système informatique ou l'extension de la recherche dans un système informatique

Le juge d'instruction est compétent pour, « *dans un but secret, intercepter, prendre connaissance, explorer et enregistrer, à l'aide de moyens techniques, des communications non accessibles au public ou des données d'un système informatique ou d'une partie de celui-ci, ou étendre la recherche dans un système informatique ou partie de celui-ci* »[244]. La notion de « communications non accessibles au public » correspond aux communications ou communications électroniques prenant place dans la sphère privée[245]. Il y a lieu d'entendre par là, « *tout énoncé, oral ou non oral, fait directement ou à distance, et notamment les déclarations et conversations directes ou téléphoniques de même que toutes les formes modernes de la télématique* »[246]. Sont par conséquent compris dans le terme de « communications non accessibles au public » , les données vocales, les textes, les images ou les signes[247]. Cette disposition permet, par conséquent, l'obtention du contenu de communications et de communications électroniques privées[248].

Il s'agit d'une mesure qui revêt un caractère exceptionnel et qui ne peut être utilisée que lorsque les nécessités de l'instruction le requièrent. De plus, il ne doit pas exister d'autres moyens d'investigation permettant la manifestation de la vérité et il faut que l'infraction

[242] Projet de loi relatif à l'amélioration des méthodes particulières de recherche et de certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications, Exposé des motifs, *Doc. parl.*, Chambre, 2015-2016, n° 54-1966/1, p. 22, 8 juillet 2016.
[243] C.i.cr., art. 39*bis*, § 5, alinéa 2.
[244] C.i.cr., art. 90*ter*, § 1er, alinéa 1er.
[245] Projet de loi relatif à l'amélioration des méthodes particulières de recherche et de certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications, Exposé des motifs, *Doc. parl.*, Chambre, 2015-2016, n° 54-1966/1, p. 53, 8 juillet 2016.
[246] Cass. (2e ch.), 26 mars 2003, *J.T.*, 2003, p. 626, cité par C. DE VALKENEER, *Manuel de l'enquête pénale*, 4e éd., Bruxelles, Larcier, 2011, p. 345.
[247] C. DE VALKENEER, *op. cit.*, p. 345.
[248] A. GOSSÉ, « Dans quelle mesure les autorités judiciaires belges peuvent-elles contraindre des entreprises de télécommunication étrangères à collaborer à une enquête pénale en Belgique ? », *Rev. dr. pén. entr.*, 2017/3, p. 184.

faisant l'objet de la mesure soit l'une des infractions énumérées au paragraphe 2 de la disposition[249]. Parmi ces infractions, nous pouvons notamment retrouver l'infraction de harcèlement téléphonique[250], de *grooming* en ligne[251], de cyberprédation[252] et les menaces pour autant qu'une plainte ait été déposée[253]. L'article 17 de la loi du 25 décembre 2016 a élargi de façon conséquente cette liste d'infractions. Il y a dès lors lieu de se questionner sur la compatibilité d'une telle extension avec la Convention de Budapest qui exige de réserver ce type de méthodes à « *un éventail d'infractions graves à définir en droit interne* »[254].

Une autre condition de mise en œuvre de cette mesure est qu'elle ne peut être effectuée qu'afin de rechercher les données qui peuvent être utiles à la manifestation de la vérité. Les seules personnes pouvant faire l'objet d'une telle mesure sont celles pour lesquelles il existe des soupçons, établis sur base d'indices précis, qu'elles aient commis l'infraction. La mesure peut également être ordonnée en ce qui concerne les moyens de communications ou systèmes informatiques que le suspect utilise régulièrement ou des lieux que celui-ci est présumé fréquenter. Enfin, la mesure peut s'appliquer à toute personne envers laquelle il existe une présomption, basée sur des faits précis, qu'elle communique régulièrement avec un suspect[255].

En vertu de cette disposition et en vue de permettre la mesure, le juge d'instruction peut ordonner, et ce, sans le consentement ou à l'insu de l'occupant, du propriétaire ou de son ayant droit ou de l'utilisateur:

- *« la pénétration dans un domicile, un lieu privé ou un système informatique ;*
- *la suppression temporaire de toute protection des systèmes informatiques concernés, le cas échéant à l'aide de moyens techniques, de faux signaux, de fausses clés ou de fausses qualités ;*
- *l'installation de dispositifs techniques dans les systèmes informatiques concernés en vue du décryptage et du décodage de données stockées, traitées ou transmises par ce système* »[256].

Par le biais de cette disposition, les enquêteurs peuvent notamment procéder au placement d'un logiciel espion sur l'ordinateur d'un individu afin de prendre connaissance du contenu

[249] C.i.cr., art. 90*ter*, § 1er, alinéa 2.
[250] C.i.cr., art. 90*ter*, § 2, 40°.
[251] C.i.cr., art. 90*ter*, § 2, 16°.
[252] C.i.cr., art. 90*ter*, § 2, 21°.
[253] C.i.cr., art. 90*ter*, § 2, 12°.
[254] Art. 21, § 1er, de la Convention du Conseil de l'Europe sur la cybercriminalité, signée à Budapest le 23 novembre 2001, *S.T.E.*, n° 185.
[255] C.i.cr., art. 90*ter*, § 1er, alinéa 4.
[256] C.i.cr., art. 90*ter*, § 1er, alinéa 3.

d'un disque dur ou d'une conversation et en prendre copie. C'est ainsi que les enquêteurs pourront avoir accès aux communications effectuées via *WhatsApp*, *Skype*, *Viber*, etc. De plus, ce logiciel peut également et, entre autres, permettre l'interception de l'ensemble des données informatiques telles que les entrées clavier, les mots de passe, les informations circulant via l'appareil et par Internet[257] [258].

Dès lors, cette mesure peut parfois porter fortement atteinte à la vie privée de l'intéressé. C'est sans doute pour cela qu'en vertu de la loi, il ne peut y avoir recours à cette mesure que pour un délai maximum d'un mois à compter de l'autorisation du juge d'instruction, sous réserve d'un ou plusieurs renouvellements d'un mois, et sans toutefois que le délai total ne puisse excéder six mois[259]. De plus, l'article 90*novies* du Code d'instruction criminelle impose au greffier d'informer par écrit la personne concernée en précisant la nature de la mesure ainsi que des dates auxquelles elle a été effectuée. Le greffier dispose d'un délai de maximum quinze jours pour effectuer la notification et ce, à partir du moment où la décision sur le règlement de procédure est devenue définitive ou à partir du moment où l'intéressé a été cité, sauf si l'identité ou l'adresse de celui-ci ne peuvent être raisonnablement trouvés[260].

Section 4. L'identification

Le procureur du Roi est compétent, en vertu de l'article 46*bis* du Code d'instruction criminelle afin de procéder ou de faire procéder à l'identification de l'abonné ou de l'utilisateur habituel d'un service de télécommunication ou du moyen de communication électronique utilisé. De plus, il peut procéder ou faire procéder à l'identification des services de communications utilisés habituellement par une personne déterminée ou ceux auxquels elle est abonnée[261].

Cette disposition ne peut être utilisée que pour obtenir des données statiques, ce qui correspond à l'ensemble des données uniques pouvant être isolées dans le temps. Cela signifie que la demande vise avant tout une cible ou une personne sans qu'il ne soit demandé d'aperçu historique des communications électroniques effectuées[262]. Cette disposition permet notamment d'obtenir des informations personnelles du détenteur d'un

[257] Projet de loi relatif à l'amélioration des méthodes particulières de recherche et de certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications, Exposé des motifs, *Doc. parl.*, Chambre, 2015-2016, n° 54-1966/1, p. 57, 8 juillet 2016.
[258] C. FORGET, « Les nouvelles méthodes d'enquête dans un contexte informatique : vers un encadrement (plus) strict », *op. cit.*, pp. 49 et 50.
[259] C.i.cr., art. 90*quater*, § 1er, alinéa 2, 4°, et 90*quinquies*, alinéa 1er.
[260] C.i.cr., art. 90*novies.*
[261] C.i.cr., art. 46*bis*, § 1er, alinéa 1er, 1° et 2°.
[262] J. KERKHOFS et P. VAN LINTHOUT, « Artikel 46*bis* van het Wetboek van strafvordering en de motiveringsplicht: de minimis non curat praetor », *T. Strafr.*, 2011/6, p. 428.

numéro de téléphone, le code PUK d'une carte SIM, la date et la durée d'activation de la carte SIM ou d'une ligne téléphonique, le compte en banque lié au rechargement d'une carte de téléphonie mobile, etc[263]. Conformément à cette disposition, le procureur du Roi a également la possibilité d'identifier le titulaire d'une adresse e-mail[264].

L'article 46*bis* du Code d'instruction criminelle peut être utilisé afin d'identifier l'utilisateur d'un réseau Internet au moyen d'un numéro d'adresse IP, mais à condition que l'adresse IP soit fixe[265]. L'adresse IP est une adresse que l'utilisateur se voit attribuer lors d'une connexion à Internet. En général, celle-ci diffère à chaque connexion et est dès lors appelée adresse IP « dynamique ». Dans le cas d'une adresse IP « dynamique », afin d'utiliser l'article 46*bis* pour identifier l'utilisateur du réseau Internet, il est nécessaire que l'adresse IP ainsi que le moment de connexion soient connus. Si le moment de la connexion n'est pas connu, il faudra, dès lors, avoir recours à l'article 88*bis* du Code d'instruction criminelle, qui sera analysé ci-après[266].

Une limitation de temps est imposée au procureur du Roi lorsque les infractions ne sont pas de nature à entraîner un emprisonnement correctionnel d'un an ou une peine plus lourde. Dans ce cas, le procureur du Roi ne pourra obtenir les données citées précédemment que pour une durée de six mois préalable à sa décision[267].

Section 5. Le repérage et la localisation

Le juge d'instruction peut, en vertu de l'article 88*bis* du Code d'instruction criminelle, faire procéder au repérage « *des données de trafic de moyens de communication électronique à partir desquels ou vers lesquels des communications électroniques sont adressées ou ont été adressées* ». Il peut également faire localiser l'origine ou la destination des communications électroniques[268]. Cette disposition vise aussi bien les communications téléphoniques que les communications par Internet[269]. Cette disposition se rapporte, contrairement à l'article 46*bis*, à l'obtention de données dynamiques. Il s'agit de données

[263] *Ibid*. ; J. KERKHOFS et P. VAN LINTHOUT, « Cybercriminaliteit doorgelicht », *T. Strafr.*, 2010/4, p. 191 ; D. VANDERMEERSCH, « Les recherches en matière de téléphonie mobile et de (télé)communications », *Colloque en droit pénal et procédure pénale*, sous la présidence de D. Bosquet, Bruxelles, Jeune barreau de Bruxelles, 2006, p. 31 ; C. DE VALKENEER, *op. cit.*, p. 363.
[264] T. HENRION, « Écoutes téléphoniques », X., *Postal Mémorialis – Lexique du droit pénal et des lois spéciales*, Malines, Kluwer, 2009, p. E43/33.
[265] D. VANDERMEERSCH, *op. cit.*, p. 31.
[266] *Ibid*. ; C. DE VALKENEER, *op. cit.*, pp. 365 et 366.
[267] C.i.cr., art. 46*bis*, § 1er, alinéa 5.
[268] C.i.cr., art. 88*bis*, § 1er, alinéa 1er.
[269] Projet de loi relatif à la collecte et à la conservation des données dans le secteur des communications électroniques, Exposé des motifs, *Doc. parl.*, Chambre, 2015-2016, n° 54-1567/1, p. 40, 11 janvier 2016.

ne pouvant être isolées à un instant précis dans le temps[270]. La mesure permet d'avoir accès au jour, à l'heure, à la durée, au correspondant ainsi qu'à la localisation de la communication,[271] mais, jamais au contenu de celle-ci[272].

Le juge d'instruction peut avoir recours à cette mesure s'il l'estime nécessaire à la manifestation de la vérité et à condition que les infractions soient susceptibles d'entraîner un emprisonnement correctionnel principal d'un an ou d'une peine plus lourde[273].

La mesure peut s'appliquer dans le futur, mais est limitée à une période de deux mois à compter de l'ordonnance, sous réserve d'un renouvellement[274]. Si la mesure porte sur une période révolue, la limitation de l'accès aux données conservées sur base de l'article 126 de la loi du 13 juin 2005 dépend de la gravité de l'infraction ayant donné lieu à ladite mesure[275]. Ces limitations dans le temps ont été introduites par l'article 9 de la loi du 29 mai 2016[276]. Le juge d'instruction bénéficie d'une durée de douze mois préalable à l'ordonnance en ce qui concerne les infractions terroristes[277]. S'agissant d'infractions visées à l'article 90*ter*, paragraphes 2 à 4, du Code d'instruction criminelle, le juge d'instruction peut exiger l'obtention des données pour une période de neuf mois préalable à l'ordonnance[278]. Tel sera notamment le cas en ce qui concerne le harcèlement téléphonique[279], le *grooming* en ligne[280], la cyberprédation[281], ainsi que les menaces à condition qu'une plainte ait été déposée[282]. Concernant les autres infractions, l'accès sera limité aux six mois précédents l'ordonnance[283].

Section 6. La cyber-infiltration

L'infiltration « virtuelle » sur Internet (notamment sur les réseaux sociaux) est régie par l'article 46*sexies* du Code d'instruction criminelle[284]. En vertu de cette disposition, les services de police peuvent être autorisés par le procureur du Roi à entretenir,

[270] J. KERKHOFS et P. VAN LINTHOUT, « Artikel 46*bis* van het Wetboek van strafvordering en de motiveringsplicht: de minimis non curat praetor », *op. cit*., p. 429.
[271] T. HENRION, *op. cit*., p. E43/21.
[272] D. VANDERMEERSCH, *op. cit*., p. 37 ; M.-A. BEERNAERT, N. COLETTE-BASECQZ, C. GUILLAIN, L. KENNES, P. MANDOUX, M. PREUMONT et D. VANDERMEERSCH, *Introduction à la procédure pénale*, 6e éd., Bruxelles, La Charte, 2017, p. 208.
[273] C.i.cr., art. 88*bis*, § 1er, alinéa 1er.
[274] C.i.cr., art. 88*bis*, § 1er, alinéa 5.
[275] M.-A. BEERNAERT, N. COLETTE-BASECQZ, C. GUILLAIN, L. KENNES, P. MANDOUX, M. PREUMONT et D. VANDERMEERSCH, *op. cit*., p. 208.
[276] Loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques, *M.B.*, 18 juillet 2016.
[277] C.i.cr., art. 88*bis*, § 2, 1er tiret.
[278] C.i.cr., art. 88*bis*, § 2, 2e tiret.
[279] C.i.cr., art. 90*ter*, § 2, 40°.
[280] C.i.cr., art. 90*ter*, § 2, 16°.
[281] C.i.cr., art. 90*ter*, § 2, 21°.
[282] C.i.cr., art. 90*ter*, § 2, 12°.
[283] C.i.cr., art. 88*bis*, § 2, 3e tiret.
[284] M.-A. BEERNAERT, H.-D. BOSLY et D. VANDERMEERSCH, *Droit de la procédure pénale*, 8e éd, tome I, Brugge, La Charte, 2017, p. 561.

éventuellement sous une identité fictive, « *des contacts sur Internet avec une ou plusieurs personnes concernant lesquels il existe des indices sérieux qu'elles commettent ou commettraient des infractions pouvant donner lieu à un emprisonnement correctionnel principal d'un an ou à une peine plus lourde* »[285]. Le recours à ce moyen est possible lors de la recherche de crimes et délits à condition que cela soit nécessaire pour l'enquête et que les autres méthodes d'investigation ne semblent pas suffisantes à la manifestation de la vérité[286].

La validité de l'autorisation, écrite et motivée (sauf en cas d'urgence)[287] du procureur du Roi est de 3 mois, sans préjudice de renouvellement[288]. Cette période limitée à tr mois pourrait être pratiquement problématique. À titre d'exemple, le délai légal prescrit sera rapidement dépassé lorsque le profil de l'enquêteur reste inactif durant une certaine période et est réutilisé par la suite[289] [290].

Les fonctionnaires de police peuvent, lors d'une opération déterminée, faire temporairement appel à l'expertise d'un individu ne faisant pas partie des services de police. Ce recours momentané doit être expressément autorisé par le procureur du Roi et doit être strictement nécessaire à la réussite de la mission[291]. Par exemple, les agents pourraient faire appel à une expertise lors d'une pénétration dans un milieu où un langage spécifique, notamment un langage de jeunes, est employé[292].

Une cause d'excuse absolutoire est prévue lorsque les fonctionnaires de police commettent des infractions strictement nécessaires dans l'exécution de leur mission de cyber-infiltration[293]. Afin d'être exemptés de peine, les fonctionnaires doivent informer par écrit et préalablement le procureur du Roi de leur intention de commettre et recevoir l'accord exprès de celui-ci[294]. De plus, « *ces infractions ne peuvent être plus graves que celles pour lesquelles la mesure est utilisée et doivent nécessairement être proportionnelles à l'objectif visé* »[295]. Si les fonctionnaires de police n'ont pas pu, préalablement, procéder à la notification au procureur du Roi, ils s'exécutent sans délai en l'informant des infractions

[285] C.i.cr., art. 46*sexies*, § 1er, alinéa 1er.
[286] C.i.cr., art. 46*sexies*, § 1er, alinéa 1er.
[287] C.i.cr., art. 46*sexies*, § 2, alinéa 2.
[288] C.i.cr., art. 46*sexies*, § 2, alinéa 1er.
[289] C.i.cr., art. 46*sexies*, § 3, alinéa 1er.
[290] C. FORGET, « Les nouvelles méthodes d'enquête dans un contexte informatique : vers un encadrement (plus) strict », *op. cit.*, p. 43.
[291] C.i.cr., art. 46*sexies*, § 1er, alinéa 3.
[292] Projet de loi relatif à l'amélioration des méthodes particulières de recherche et de certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications, Exposé des motifs, *Doc. parl.*, Chambre, 2015-2016, n° 54-1966/1, p. 38, 8 juillet 2016.
[293] O. MICHIELS et G. FALQUE, *op. cit.*, p. 196.
[294] C.i.cr., art. 46*sexies*, § 3, alinéas 1 et 5.
[295] C.i.cr., art. 46*sexies*, § 3, alinéa 2.

commises, et procèdent ensuite à une confirmation par écrit[296]. Cette exemption de peine, sous réserve de l'accord exprès du procureur du Roi, s'applique également aux infractions commises par les personnes ayant apporté leur aide directe ou leur assistance nécessaire à l'exécution de l'infiltration sur Internet ainsi qu'aux personnes consultées afin de procéder à une expertise[297]. Aucune précision quant au type d'infractions admissibles ne peut être trouvée dans la loi. De plus, les infractions pouvant être commises ne se limitent pas au « cyberespace ». Ceci entre donc en contradiction avec l'avis du Conseil d'État du 9 mai 2016[298].

La disposition n'est pas d'application lorsque les services de police, sans utiliser une identité fictive crédible, interagissent personnellement sur Internet avec un ou plusieurs individus et lorsque le but direct est de procéder à une arrestation ou d'effectuer une vérification ciblée[299]. D'après la Commission de protection de la vie privée, cette exclusion n'est pas suffisamment claire et devrait être encadrée de façon distincte dans le Code d'instruction criminelle ou dans la loi sur la fonction de police. Cela permettrait que les principes de légitimité et de prévisibilité soient respectés[300]. Cependant, la Cour de cassation, par un arrêt du 28 mars 2017, a considéré que l'article 26 de la loi sur la fonction de police[301] constitue une base légale suffisante afin que les services de police puissent « patrouiller » sur Internet sur les « sources ouvertes » ou « semi-publiques »[302]. L'article 26 de la loi sur la fonction de police autorise, en effet, les fonctionnaires de police à pénétrer dans des lieux accessibles au public afin de rechercher les infractions telles que les crimes, délits et contraventions, d'en récolter les preuves et de livrer les auteurs de ces infractions aux tribunaux afin qu'ils soient punis[303].

[296] C.i.cr., art. 46*sexies*, § 3, alinéa 6.
[297] C.i.cr., art. 46*sexies*, § 3, alinéa 3.
[298] 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, Avis du Conseil d'État, *Doc. parl*., Chambre, 2015-2016, n° 54-1966/1, pp. 135 à 137, 8 juillet 2016.
[299] C.i.cr., art. 46*sexies*, § 1er, alinéa 4.
[300] 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, Avis de la Commission vie privée, *Doc. parl*., Chambre, 2015-2016, n° 54-1966/2, pp. 31 à 32, 11 juillet 2016.
[301] Loi du 5 août 1992 sur la fonction de police, *M.B.*, 22 décembre 1992.
[302] Cass. (2e ch.), 28 mars 2017, R.G. n° P.16.1245.N, p. 4.
[303] C.i.cr., art. 8.

Chapitre 3. Les obligations de collaboration

Section 1. L'obligation de collaboration des opérateurs de réseaux de communications électroniques et des services, sur le territoire belge, permettant la transmission de signaux au moyen des réseaux de communications électroniques ou autorisant les utilisateurs à obtenir, recevoir ou diffuser des informations à l'aide d'un réseau de communications électroniques

Auparavant, seul l'opérateur d'un réseau de communications électroniques ainsi que le fournisseur d'un service de communications électroniques pouvaient être contraints de collaborer à l'enquête pénale. La loi du 25 décembre 2016 a élargi la définition de la notion de « fournisseur de communications électroniques » en la remplaçant par « *toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques* »[304]. Par souci de clarté, la loi de décembre 2016 a ajouté à cette définition qu' « *est également compris le fournisseur d'un service de communications électroniques* ». Cette définition est tirée de l'arrêt de la Cour de cassation du 18 janvier 2011, dénommé « Yahoo », que nous analyserons ci-après[305]. Cette catégorie de fournisseurs doit être interprétée très largement et la nouvelle définition légale englobe par conséquent les entreprises telles que *Yahoo Mail*, *Hotmail*, *Gmail,* mais également les services comme *Facebook*, *Twitter*, *WhatsApp*, *Instagram*, etc[306].

1. *L'identification de l'abonné ou de l'utilisateur habituel du service ou du moyen de communication électronique ou l'identification des services de communications utilisés*

Si nécessaire, le procureur du Roi peut, en vertu de l'article 46*bis* du Code d'instruction criminelle, requérir le concours d'opérateurs de réseaux de communications électroniques[307]. Cette obligation de collaboration s'étend également aux services, sur le

[304] Projet de loi relatif à l'amélioration des méthodes particulières de recherche et de certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications, Exposé des motifs, *Doc. parl.*, Chambre, 2015-2016, n° 54-1966/1, p. 32, 8 juillet 2016.
[305] Cass. (2e ch.), 18 janvier 2011, R.G. n° P.10.1347.N.
[306] Projet de loi relatif à l'amélioration des méthodes particulières de recherche et de certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications, Exposé des motifs, *Doc. parl.*, Chambre, 2015-2016, n° 54-1966/1, pp. 32 et 33, 8 juillet 2016.
[307] C. FORGET, « La collecte de preuves informatiques en matière pénale », *Pas de droit sans technologie*, sous la direction de J.-F. Henrotte et F. Jongen, vol. 158, CUP, Bruxelles, Larcier, 2015, p. 265.

territoire belge, permettant la transmission de signaux au moyen des réseaux de communications électroniques ou autorisant les utilisateurs à obtenir, recevoir ou diffuser des informations à l'aide d'un réseau de communications électroniques[308]. Cette collaboration a pour but de permettre l'identification de l'abonné ou de l'utilisateur habituel d'un service de télécommunication ou du moyen de communication électronique utilisé[309] [310]. De plus, elle permet d'identifier les services de communications utilisés habituellement par une personne déterminée ou ceux auxquels elle est abonnée[311] [312].

Toute personne qui refuse de prêter son concours, ne le prête pas en temps réel ou au moment précisé dans la réquisition peut se voir infliger une amende allant de vingt-six euros à dix mille euros[313].

Concernant cette disposition, il est intéressant d'analyser l'affaire *Yahoo* qui a fait couler beaucoup d'encre. En l'espèce, le procureur du Roi de Termonde a ouvert, en 2007, une information pénale visant plusieurs infractions commises au préjudice d'une entreprise commerciale belge au moyen d'adresses e-mail utilisées par les auteurs afin de commettre les faits et attribuées par la société américaine *Yahoo*[314]. Le procureur du Roi a, dès lors, exigé que *Yahoo* collabore sur base de l'article 46*bis* du Code d'instruction criminelle en vue de l'obtention de l'ensemble des données d'identification et d'enregistrement des personnes ayant procédé à la création ou à l'enregistrement du compte e-mail, de l'adresse e-mail liée au profil ainsi que les autres données personnelles ou informations pouvant être utiles afin d'identifier l'utilisateur du compte[315]. L'entreprise américaine, ne possédant pas de siège sur le territoire belge, a refusé de prêter son concours, car, selon elle, les informations sollicitées étaient soumises à l'*Electronic Communications Privacy Act*, et étaient, par conséquent, sous la protection de la législation américaine[316]. D'après *Yahoo*, les autorités judiciaires belges devaient, au moyen d'une commission rogatoire internationale, s'adresser au *US Departement of Justice*[317] [318].

[308] C.i.cr., art. 46*bis*, § 1er, alinéa 2, 2e tiret.
[309] C.i.cr., art. 46*bis*, § 1er, alinéa 1er, 1°.
[310] A. GOSSÉ, *op. cit*., p. 182.
[311] C.i.cr., art. 46*bis*, § 1er, alinéa 1er, 2°.
[312] C. DE VALKENEER, *op. cit*., p. 363.
[313] C.i.cr., art. 46*bis*, § 2, alinéa 4.
[314] L. KERZMANN, « L'affaire Yahoo! Ou à qui s'adresse l'obligation de collaboration instaurée par l'article 46*bis* du Code d'instruction criminelle ? », *R.D.T.I*., n° 44, 2011, p. 116 ; R. ROEX, « Belgische justitie kan rechtstreeks informatie opvragen van Amerikaanse techreuzen », *Juristenkrant*, 2015, n° 319, p. 5 ; O. LEROUX, « Arnaques, fraudes et escroqueries sur internet : moyens concrets d'investigation. Point sur l'affaire dite Yahoo! À la suite du second arrêt de la Cour de cassation », *J.T*., 2012/40-41, n° 6500, p. 841.
[315] Corr. Flandre orientale (div. Termonde), 2 mars 2009, *T. Strafr*., 2009/2, p. 118.
[316] O. LEROUX, « Arnaques, fraudes et escroqueries sur internet : moyens concrets d'investigation. Point sur l'affaire dite Yahoo! À la suite du second arrêt de la Cour de cassation », *op. cit*., p. 841 ; C. DE VALKENEER, *op. cit*., p. 366.
[317] Corr. Flandre orientale (div. Termonde), 2 mars 2009, *T. Strafr*., 2009/2, p. 118.
[318] O. LEROUX, « Arnaques, fraudes et escroqueries sur internet : moyens concrets d'investigation. Point sur l'affaire dite Yahoo! À la suite du second arrêt de la Cour de cassation », *op. cit*., p. 841.

Face au refus de *Yahoo* de prêter son concours, le ministère public l'a assigné devant le tribunal correctionnel de Termonde sur base de l'article 46*bis*, paragraphe 2, alinéa 4, du Code d'instruction criminelle[319]. Le tribunal a rendu son jugement le 2 mars 2009 et a condamné la société américaine. Selon le tribunal, malgré que l'entreprise soit de nationalité américaine, elle constitue un fournisseur de services de communications électroniques présent de manière virtuelle et économique en Belgique et doit ainsi être considérée comme judiciairement présente sur le territoire belge. Par conséquent, *Yahoo* est dans l'obligation de collaborer en vertu de l'article 46*bis* du Code d'instruction criminelle, d'autant plus qu'aucune distinction n'est créée par cette disposition en fonction de l'immatriculation ou de la nationalité de l'opérateur ou du fournisseur de services. Le tribunal a considéré que la législation américaine ne pouvait s'appliquer au trafic de données prenant place en Belgique et ne pouvait porter atteinte à la souveraineté belge en ce qui concerne le droit pénal et la procédure pénale[320].

Yahoo a interjeté appel et la Cour d'appel de Gand a réformé le jugement du tribunal correctionnel de Termonde par un arrêt du 30 juin 2010[321]. Le débat portait sur le fait de savoir si *Yahoo* pouvait être considéré comme un opérateur de réseau de communications électroniques ou un fournisseur de services de communications électroniques au sens de l'article 46*bis* du Code d'instruction criminelle (précédemment à la modification de la notion de fournisseur apportée par la loi du 25 décembre 2016). La cour a considéré que pour répondre à cette question, il fallait se référer au sens donné à ces notions par la loi du 13 juin 2005[322]. Par son arrêt, la cour a acquitté *Yahoo* en décidant qu'il n'était pas obligé de collaborer conformément à l'article 46*bis,* car il n'entrait pas dans les notions d'opérateur et de fournisseur au sens de la loi précitée[323].

Considérant que le principe de l'autonomie conceptuelle du droit pénal avait été méconnu et que la notion de fournisseur d'un service de communications électroniques avait été interprétée de façon erronée, le parquet général de Gand a introduit un pourvoi en cassation contre l'arrêt de la Cour d'appel[324]. La Cour de cassation, par son arrêt du 18 janvier 2011, a conclu que la notion de fournisseur au sens de l'article 46*bis*, devant être entendue comme « *quiconque (qui) dispense des services de communications électroniques, comme notamment la transmission de données de communication* »[325].

---

[319] L. KERZMANN, *op. cit.*, p. 117 ; O. LEROUX, « Arnaques, fraudes et escroqueries sur internet : moyens concrets d'investigation. Point sur l'affaire dite Yahoo! À la suite du second arrêt de la Cour de cassation », *op. cit.*, p. 841.
[320] Corr. Flandre orientale (div. Termonde), 2 mars 2009, *T. Strafr.*, 2009/2, p. 116.
[321] Gand (3e ch.), 30 juin 2010, *T. Strafr.*, 2011/22, p. 132.
[322] C. FORGET, « La collecte de preuves informatiques en matière pénale », *op. cit.*, p. 266.
[323] O. LEROUX, « Arnaques, fraudes et escroqueries sur internet : moyens concrets d'investigation. Point sur l'affaire dite Yahoo! À la suite du second arrêt de la Cour de cassation », *op. cit.*, p. 842.
[324] *Ibid*. ; L. KERZMANN, *op. cit.*, p. 119.
[325] Cass. (2e ch.), 18 janvier 2011, R.G. n° P.10.1347.N, p. 4.

Cette notion est plus large que celle d'opérateur contenue dans la loi précitée[326]. Partant, la Cour de cassation a décidé de casser l'arrêt de la Cour d'appel de Gand et a renvoyé l'affaire devant la juridiction du second degré de Bruxelles[327].

La Cour d'appel de Bruxelles a estimé, dans un arrêt du 12 octobre 2011, que le ministère public ne disposait pas du pouvoir juridictionnel pour exercer ses fonctions extra-territorialement. Puisque la société *Yahoo* n'a pas été requise régulièrement, la cour a conclu qu'elle n'avait pas manqué à ses obligations relevant de l'article 46*bis*, paragraphe 2 en ne collaborant pas suite au réquisitoire du procureur du Roi[328] [329].

Suite à cet arrêt, un nouveau pourvoi en cassation a été introduit par le procureur général. La Cour de Cassation, dans son arrêt du 4 septembre 2012, a cassé l'arrêt de la Cour d'appel de Bruxelles. D'après la Cour de cassation, un réquisitoire ne peut être considéré comme irrégulier par le seul fait que le procureur du Roi ait expédié celui-ci à partir de la Belgique vers l'adresse d'un opérateur ou d'un fournisseur établi à l'étranger[330] [331].

L'affaire a dès lors été renvoyée devant la Cour d'appel d'Anvers[332] qui a confirmé, par un arrêt rendu le 20 novembre 2013, le jugement du tribunal correctionnel de Termonde datant du 2 mars 2009[333]. La cour a décidé que la société est dans l'obligation de prêter son concours en vertu de l'article 46*bis* du Code d'instruction criminelle puisqu'elle est présente sur le territoire belge et offre des services e-mail gratuits.

Après un pourvoi, introduit cette fois par *Yahoo*, la Cour de cassation a rendu un dernier arrêt le 1er décembre 2015 et a ainsi clôturé cette affaire tumultueuse[334]. La cour a considéré qu'il était possible pour le procureur du Roi de faire appel, directement, à des fournisseurs de services étrangers pour que ceux-ci collaborent[335], étant donné que leurs activités économiques sont activement destinées au consommateur belge[336].

---

[326] R. ROEX, « Belgische justitie kan rechtstreeks informatie opvragen van Amerikaanse techreuzen », *op. cit.*, p. 5.
[327] Cass. (2e ch.), 18 janvier 2011, R.G. n° P.10.1347.N, pp. 5 et 6.
[328] Bruxelles (13e ch.), 12 octobre 2011, *A&M*, 2012/2-3, pp. 238 et 239.
[329] O. LEROUX, « Arnaques, fraudes et escroqueries sur internet : moyens concrets d'investigation. Point sur l'affaire dite Yahoo! À la suite du second arrêt de la Cour de cassation », *op. cit.*, p. 842.
[330] Cass. (2e ch.), 4 septembre 2012, *T. Strafr.*, 2012/6, p. 464.
[331] O. LEROUX, « Arnaques, fraudes et escroqueries sur internet : moyens concrets d'investigation. Point sur l'affaire dite Yahoo! À la suite du second arrêt de la Cour de cassation », *op. cit.*, p. 842.
[332] Anvers (12e ch.), 20 novembre 2013, *T. Strafr.*, 2014/1, p. 73.
[333] K. DE SCHEPPER, « Cassatie bevestigt: Belgische gerecht kan rechtstreeks gegevens vorderen van Yahoo », *R.A.B.G.*, 2016/7, p. 490.
[334] Cass. (2e ch.), 1er décembre 2015, R.G. n° P.13.2082.N.
[335] R. ROEX, « De Yahoo-zaak: Belgische justitie plant vlag in cyberspace », *Vigiles*, 2016/2, p. 69.
[336] Cass. (2e ch.), 1er décembre 2015, R.G. n° P.13.2082.N, p. 4.

2. *Le repérage et la localisation des communications électroniques*

Si cela s'avère nécessaire, le juge d'instruction peut, en vertu de l'article 88*bis* du Code d'instruction criminelle, exiger la collaboration des acteurs cités ci-avant[337]. Cette collaboration peut être utile afin de repérer « *des données de trafic de moyens de communication électronique à partir desquels ou vers lesquels des communications électroniques sont adressées ou ont été adressées* »[338]. Elle peut également s'avérer nécessaire afin de localiser l'origine ou la destination des communications électroniques[339].

Une amende allant de vingt-six euros à dix mille euros sera infligée, à l'instar de l'article 46*bis*, à toute personne refusant de prêter son concours, ne le prêtant pas en temps réel ou au moment précisé dans la réquisition[340].

3. *L'interception, la prise de connaissance, l'exploration et l'enregistrement, dans un but secret, de communications non accessibles au public ou des données d'un système informatique ou, l'extension de la recherche dans un système informatique*

En vertu des articles 90*ter* et suivants du Code d'instruction criminelle, le juge d'instruction peut, exiger le concours des acteurs cités ci-avant[341]. Ceux-ci peuvent, dans un but secret, se voir obligés de collaborer afin d'intercepter, prendre connaissance, explorer et enregistrer des communications non accessibles au public ou des données d'un système informatique ou partie de celui-ci ainsi que d'étendre la recherche dans un système informatique ou partie de celui-ci[342]. Une amende allant de vingt-six euros à vingt mille euros sera infligée à toute personne refusant de prêter son concours technique, ne le prêtant pas en temps réel ou, le cas échéant, au moment indiqué dans la réquisition[343].

Section 2. Les obligations de collaboration des personnes présumées disposer d'une connaissance particulière ou des personnes appropriées

Deux types de collaboration sont prévus par l'article 88*quater* du Code d'instruction criminelle. La première est une obligation d'information alors que la deuxième est une

[337] C.i.cr., art. 88*bis*, § 1er, alinéa 1er, 1°.
[338] C.i.cr., art. 88*bis*, § 1er, alinéas 1er et 2.
[339] C.i.cr., art. 88*bis*, § 1er, alinéa 1er, 2°.
[340] C.i.cr., art. 88*bis*, § 4, alinéa 3.
[341] C.i.cr., art. 90*quater*, § 2, alinéa 1er.
[342] C.i.cr., art. 90*ter*, § 1er, alinéa 1er.
[343] C.i.cr., art. 90*quater*, § 2, alinéa 3.

obligation « d'action ». Il existe également une obligation de coopération en vertu de l'article 99*quater*, paragraphe 4, du même Code.

1. *L'obligation d'information et l'obligation d' « intervention »*

Ces deux types de collaboration relèvent de la compétence du juge d'instruction ou de celle d'un officier de police judiciaire auxiliaire du procureur du Roi et de l'auditeur du travail délégué par lui.

Le premier type de collaboration est une obligation d'information incombant à toute personne présumée disposer d'une connaissance particulière du système informatique faisant l'objet d'une recherche ou de son extension. Cette obligation de collaboration s'étend également aux personnes présumées disposer d'une connaissance particulière des services permettant la protection ou le cryptage des données étant « *stockées, traitées ou transmises par un système informatique* »[344]. Le juge d'instruction peut donc enjoindre à ces personnes de fournir, dans une forme compréhensible, « *des informations sur le fonctionnement de ce système et sur la manière d'y accéder ou d'accéder aux données qui sont stockées, traitées ou transmises par un tel système* »[345]. Il pourra, par conséquent, leur être demandé de communiquer un mot de passe, une clé de cryptage, de décrire les mesures de sécurité servant de protection au système informatique, etc.

Concernant le deuxième type de collaboration, il s'agit d'une obligation d'intervention à l'égard de toute personne appropriée. Il peut être enjoint à ces personnes de faire fonctionner le système informatique ou de « *rechercher, rendre accessibles, copier, rendre inaccessibles ou retirer les données pertinentes qui sont stockées, traitées ou transmises par ce système* », et ce, dans la forme demandée[346]. Cette obligation est une obligation de moyens de nature technique[347].

Les personnes concernées par cet article 88*quater* ne sont pas précisément définies. De nombreuses personnes sont, dès lors, susceptibles de devoir collaborer telles que, par exemple, l'informaticien chargé du système informatique qui fait l'objet de la mesure ou l'opérateur d'un réseau de communications électroniques[348].

---

[344] C.i.cr., art. 88*quater*, § 1er.
[345] C.i.cr., art. 88*quater*, § 1er.
[346] C.i.cr., art. 88*quater*, § 2, alinéa 1er.
[347] O. Leroux, « Criminalité informatique spécifique », *Les infractions,* 2e éd., vol. 1 : Les infractions contre les biens , Bruxelles, Larcier, 2016, p. 507.
[348] *Ibid*.

En cas de défaut de collaboration, un emprisonnement de six mois à trois ans et une amende de vingt-six à vingt mille euros ou l'une de ces peines seulement pourra être infligée. Si cette collaboration non fournie aurait pu empêcher la commission d'un crime ou d'un délit ou en limiter les effets, les sanctions pénales pourront être portées à un emprisonnement allant d'un à cinq ans et d'une amende de cinq cents à cinquante mille euros[349].

2. *Cette obligation d'information s'étend-elle à l'inculpé ?*

Contrairement à l'obligation d'intervention qui ne peut concerner ni l'inculpé ni ses ascendants, descendants, frères, sœurs, conjoints et alliés, il n'existe aucune précision quant à l'obligation d'information[350]. Plusieurs juridictions se sont prononcées à ce sujet. Le tribunal correctionnel de Termonde, a, dans son jugement datant du 17 novembre 2014, considéré qu'il est interdit d'obliger un suspect à collaborer de manière active avec les autorités poursuivantes. D'après le tribunal, si le prévenu est enjoint de donner l'accès aux supports de données, il est dès lors, au moyen d'une prestation intellectuelle personnelle, contraint de coopérer activement à l'administration de la preuve. Par conséquent, les éléments de preuve recueillis à l'aide des supports de données cryptées doivent être frappés de nullité[351]. La Cour d'appel de Gand a confirmé cette approche dans un arrêt du 23 juin 2015[352]. En effet, « *le droit de ne pas contribuer à sa propre incrimination et le droit de garder le silence sont des normes internationales généralement reconnus qui sont au cœur de la notion de procès équitable* »[353].

Toutefois, le 21 décembre 2017, la Cour d'appel d'Anvers, chambre des mises en accusation, a opéré un revirement de jurisprudence. Elle a considéré que le fait qu'un juge d'instruction ait la faculté d'ordonner à l'inculpé, sous peine d'être pénalement sanctionné, de divulguer le code pin de son smartphone pour que les enquêteurs puissent procéder à l'exploitation des données stockées, était compatible avec le droit à un procès équitable[354]. La cour s'est référée, tout comme les travaux préparatoires[355], à l'arrêt *Saunders* de la Cour européenne des droits de l'homme. Dans ce fameux arrêt, la juridiction de Strasbourg a considéré que restait en dehors du champ d'application du droit au silence le fait d'obtenir des données de la part de l'accusé en ayant recours à des pouvoirs coercitifs, lorsque celles-ci existent indépendamment de sa volonté. Nous pouvons retrouver d'autres

[349] C.i.cr., art. 88*quater*, § 3.
[350] C.i.cr., art. 88*quater*, § 2, alinéa 2.
[351] Corr. Flandre orientale (div. Termonde), 17 novembre 2014, *T. Strafr.*, 2016/3, pp. 255 à 260.
[352] Gand, 23 juin 2015, *N.J.W.*, 2016/3, n° 336, p. 134, note C. Conings.
[353] Cour eur. D.H., arrêt Brusco c. France, 14 octobre 2010, req. n° 1466/07, § 44.
[354] Anvers (mis. acc.), 21 décembre 2017, inédit, R.G. n° K.2895.2017.
[355] Projet de loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl.*, Chambre, 1999-2000, n° 50-213/1, p. 27, 3 novembre 1999.

exemples de données qui sont indépendantes de la volonté de l'accusé tels que les documents recueillis au moyen d'un mandat, les empreintes ADN, l'haleine, le sang ou l'urine[356].

Cette interprétation peut être nuancée puisque contrairement aux documents fiscaux tenus conformément à une obligation légale et pouvant être saisis, lors, notamment, d'une perquisition, la création d'un mot de passe se fait sur base de l'initiative de son auteur. Dès lors, un mot de passe devrait être protégé par le droit au silence[357]. Le droit au silence n'englobe pas uniquement le droit de se taire, mais également celui de l'accusé ne pas avoir à donner des informations pouvant affecter sensiblement sa position ou faciliter son incrimination[358]. Ce droit pourrait donc être violé lorsque le suspect se voit obligé de fournir l'accès aux données stockées dans son téléphone portable[359].

Avec l'avancée des technologies, l'authentification peut désormais se faire également par l'introduction d'une empreinte digitale ou d'une reconnaissance faciale. Dès lors, l'intéressé pourrait se voir contraint de collaborer puisque dans ce cas, les données existent indépendamment de sa volonté. Néanmoins, si le suspect est contraint physiquement, par les autorités, à collaborer, l'usage de pouvoirs coercitifs doit être encadré[360]. D'après la Cour européenne des droits de l'homme, une série de facteurs doivent être examinés afin de déterminer si un tel dispositif est compatible avec le droit au silence. Les facteurs à analyser sont les suivants : « *la nature et le degré de la coercition employée pour l'obtention des éléments de preuve ; le poids de l'intérêt public à la poursuite de l'infraction en question et à la sanction de son auteur ; l'existence de garanties appropriées dans la procédure et l'utilisation faite des éléments ainsi obtenus* »[361].

3. *L'obligation de fournir des informations sur le fonctionnement d'un moyen de communication ou d'un système informatique et sur la manière d'accéder à son contenu*

Toute personne présumée disposer d'une connaissance particulière du moyen de communication ou du système informatique faisant l'objet de la mesure visée à l'article 90*ter*, alinéa 1er, du Code d'instruction criminelle peut être obligée par le juge d'instruction à prêter son concours. Sont également visées par cette obligation les personnes présumées

[356] Cour eur. D.H., arrêt Saunders c. Royaume-Uni, 17 décembre 1996, req. n° 1187/91, § 69.
[357] Cour eur. D.H., arrêt Funke c. France, 25 février 1993, req. n° 110588/83.
[358] C. FORGET, « Méthodes d'enquête pénales et protection des personnes vulnérables dans l'environnement numérique », *Vulnérabilités et droits dans l'environnement numérique*, Bruxelles, Larcier, 2018, pp. 199 et 200.
[359] C. FORGET, « Les nouvelles méthodes d'enquête dans un contexte informatique : vers un encadrement (plus) strict », *op. cit.*, p. 47.
[360] C. FORGET, « Méthodes d'enquête pénales et protection des personnes vulnérables dans l'environnement numérique », *op. cit.*, p. 201.
[361] Cour eur. D.H., arrêt Jalloh c. Allemagne, 11 juillet 2006, req. n° 54810/00, § 117.

avoir une connaissance particulière en ce qui concerne les services ou applications permettant de « *protéger, de coder ou de crypter les données qui sont stockées, traitées ou transmises par un moyen de communication ou un système informatique* »[362]. Cette collaboration consiste à fournir des informations sur le fonctionnement du moyen de communication ou du système informatique ainsi que sur la manière d'accéder, dans une forme compréhensible ou dans la forme souhaitée par le juge d'instruction, au contenu étant ou ayant été transmis[363]. En cas de refus de collaborer, un emprisonnement de six mois à un an ainsi qu'une amende allant de vingt-six euros à vingt mille euros ou l'une de ces deux peines pourra être infligée[364].

Une affaire récente illustre la difficulté de définir une limite à l'étendue de l'obligation de collaboration. La Cour d'appel d'Anvers a rendu un arrêt le 15 novembre 2017[365], à la suite d'un jugement de condamnation du tribunal correctionnel d'Anvers du 27 octobre 2016[366]. Ces deux décisions sont relatives à une ordonnance prise par le juge d'instruction de Malines sur base des articles 88*bis* et 90*quater* du Code d'instruction criminelle. Cette ordonnance avait pour objet d'obliger *Skype* à collaborer afin d'intercepter des données de communications électroniques. *Skype* a refusé en invoquant qu'il lui était matériellement impossible de prêter son concours, car les données sont chiffrées depuis le destinateur et déchiffrées une fois parvenues chez le destinataire. Par son arrêt, la Cour d'appel d'Anvers a considéré que l'entreprise était tenue et aurait dû prendre en considération, lors de la création de ses services, les obligations de collaboration existantes en droit belge.

Contrairement à l'article 88*quater*, paragraphe 2, du Code d'instruction criminelle qui oblige les tiers à collaborer dans les limites de leurs moyens, aucune dérogation n'est prévue à l'article 90*quater* du même Code. C'est pourquoi la cour a déduit que l'article 90*quater* du Code d'instruction criminelle impose une obligation positive vis-à-vis des tiers, et ce dès le moment où l'application est conçue[367]. Cette jurisprudence a été confirmée par la Cour de cassation dans un arrêt du 19 février 2019[368].

Chapitre 4. Federal et Regional Crime Units

La Federal (FCCU) et les Regional (RCCU) Computer Crime Units désignent les services de police spécialisés dans l'analyse de systèmes informatiques et de télécommunications. Ces

[362] C.i.cr., art. 90*quater*, § 4, alinéa 1er.
[363] C.i.cr., art. 90*quater*, § 4, alinéas 1er et 2.
[364] C.i.cr., art. 90*quater*, § 4, alinéa 3.
[365] Anvers (4e ch.), 15 novembre 2017, inédit, R.G. n° C.1288.2017.
[366] Corr. Anvers (div. Malines), 27 octobre 2016, *N.J.W.*, 2016/20, pp. 921 à 928.
[367] C. FORGET, « Les nouvelles méthodes d'enquête dans un contexte informatique : vers un encadrement (plus) strict », *op. cit.*, p. 51.
[368] Cass. (2e ch.), 19 février 2019, R.G. n° P.17.1229.N, p. 5.

unités ont différentes missions. Tout d'abord, elles assistent efficacement et de façon opportune les services de police à l'occasion de dossiers judiciaires. Cette assistance a pour but de détecter, conserver et procurer aux enquêteurs, dans un format lisible, l'ensemble des données pertinentes dans le cadre des technologies de l'information et de la communication (ICT). Ensuite, elles luttent efficacement, au moyen de la spécialisation, de la prévention et des interventions proactives, afin de limiter au maximum l'impact néfaste de la criminalité informatique sur la vie sociale des citoyens.

La FCCU est une entité au niveau national, composée de trois sections et faisant partie de la Direction centrale de la lutte contre la criminalité grave et organisée. La FCCU est chargée de lutter contre la criminalité concernant les ICT afin, notamment, de protéger les citoyens des nouvelles formes de cybercriminalité. Il pourra être fait appel à la FCCU pour analyser légalement les grands réseaux, les systèmes informatiques centraux. De plus, l'aide de cette unité pourra être requise dans le cadre d'une analyse approfondie concernant la criminalité ICT.

Trois hypothèses peuvent se présenter lorsque la FCCU traite les dénonciations reçues. La première hypothèse est celle où une infraction pénale est constatée. Lorsque la Belgique est compétente pour cette infraction, un procès-verbal initial sera rédigé et envoyé au parquet compétent. Dans le cas contraire, lorsque la compétence revient à une autorité judiciaire étrangère, le service de police étranger en est averti par Interpol. Le deuxième cas de figure est la situation où la FCCU est informée d'un phénomène ou d'une enquête pénale qui est déjà en cours. Dès lors, la FFCU procède à la communication de l'information reçue au service de police belge compétent. Dans la dernière hypothèse, lorsqu'il s'agit d'une infraction administrative, la FCCU informe, s'il y en a une, l'autorité belge compétente.

Concernant les RCCU, il y en a une par arrondissement judiciaire. Ces unités ont pour mission, sous la direction des directeurs judiciaires, de procéder aux analyses légales des ICT de divers supports de données tels que les ordinateurs ainsi que les petits réseaux. Elles sont chargées d'identifier les auteurs des faits[369].

En avril 2018, la FCCU faisait état, d'un manque considérable de membres du personnel. Cette entité, devant normalement compter 44 « cyberflics », n'en comptabilisait que 22. D'après le directeur de cette unité, Walter Coenraets, cette problématique va s'accentuer

[369] X., « Federal Computer Crime Unit », 2019, *Police Fédérale*, disponible sur https://www.police.be/5998/fr/a-propos/directions-centrales/federal-computer-crime-unit (28 juillet 2019).

dramatiquement et à court terme. Il est donc probable que celle-ci ne puisse plus exercer son travail.

D'après le co-président de l'Association des juges d'instruction de Belgique, Philippe Van Linthout, cette problématique ne concerne pas uniquement les FCCU, mais également les RCCU. Selon lui, « *les enquêtes sont à l'arrêt et en retard depuis des mois. Comme l'usage de smartphones et autres appareils du genre a explosé dans notre société, il faut presque toujours une enquête ICT et lire les données. Quand il faut attendre 3, 4, 5 ou même 6 mois pour avoir les résultats, c'est très frustrant surtout si des gens doivent être arrêtés dans un dossier* »[370].

[370] S. ENGLER, « La Federal Computer Crime Unit manque de personnel », 30 avril 2018, *RTBF*, disponible sur https://www.rtbf.be/info/belgique/detail_la-federal-computer-crime-unit-manque-de-personnel?id=9906286 (2 août 2019).

Conclusion

Le cyber-harcèlement dont il n'existe pas de définition unique peut prendre plusieurs formes. Ce phénomène en voie d'expansion peut engendrer des conséquences désastreuses. C'est pourquoi une lutte efficace à l'encontre de cette problématique doit être mise en place. L'Union européenne, par diverses approches tente de sensibiliser ses citoyens aux nouvelles technologies de l'information et de la communication et aux dérives qu'elles peuvent engendrer.

Au vu des statistiques contenues dans le Moniteur de sécurité de 2018 publié par la Police Fédérale, un très grand nombre d'infractions liées à la cybercriminalité ne font pas l'objet de plainte à la police. Il est donc nécessaire de faciliter le dépôt de cette plainte et de sensibiliser et spécialiser les policiers à cette nouvelle forme de criminalité afin qu'il puisse être donné suite à la plainte déposée.

Quelle est la situation juridique actuelle au niveau belge en ce qui concerne le harcèlement en ligne ? Les dispositions législatives existantes permettent-elles une incrimination et une poursuite efficace des auteurs de ces agissements?

Comme nous l'avons vu dans cet exposé, le Code pénal n'incrimine pas le cyber-harcèlement en tant que tel. Néanmoins, certaines formes d'expression constitutives de cyber-harcèlement sont encadrées juridiquement par le droit pénal. Certains comportements restent néanmoins impunis et appellent à une réaction législative. Malgré plusieurs propositions de loi déposées en vue d'incriminer le comportement d'*happy slapping*[371], celui-ci n'a toujours pas fait l'objet d'une incrimination spécifique par le législateur belge. Tel est également le cas en ce qui concerne l'incitation au suicide. Cela démontre un certain retard législatif puisque ces deux agissements font l'objet, chez nos voisins français, d'une incrimination propre[372].

De plus, il serait judicieux, selon nous, de modifier l'article 145, paragraphe 3*bis*, de la loi du 13 juin 2005 incriminant le harcèlement téléphonique en l'adaptant aux évolutions technologiques actuelles. Par exemple, il pourrait être opportun de prévoir un cas

[371] Proposition de loi visant à réprimer le *happy slapping*, *Doc. parl*., Chambre, 2006-2007, n° 51-3079/1, 13 avril 2007 ; Proposition de loi visant à réprimer le *happy slapping*, *Doc. parl*., Chambre, 2007-2008, n° 52-497/1, 4 décembre 2007 ; Proposition de loi visant à réprimer le *happy slapping*, *Doc. parl*., Chambre, 2010-2011, n° 53-417/1, 19 octobre 2010.
[372] C. pén., art. 222-33-3 et 223-13.

spécifique applicable aux réseaux sociaux. Il serait également nécessaire de supprimer la condition de correspondance puisque de nombreux messages sont postés au travers des réseaux sociaux, sans prendre place lors d'un échange ou d'une communication avec la victime.

Dans de nombreux cas, le cyber-harcèlement touche des personnes mineures, aussi bien en tant qu'auteurs qu'en tant que victimes. C'est pourquoi, il est urgent et fondamental, de sensibiliser, conscientiser et responsabiliser, de manière préventive, les élèves, leurs parents et professeurs à cette problématique et plus largement, à celle de la cybercriminalité. Afin de parvenir à cet objectif, diverses solutions peuvent être envisagées. Tout d'abord, des cours relatifs aux médias pourraient être enseignés dans les écoles. Ensuite, les parents pourraient réguler l'accès de leurs enfants sur Internet et échanger avec eux sur la nature de leurs activités en ligne. Enfin, des temps de parole pourraient être mis en place dans les écoles, auprès d'un interlocuteur unique afin que l'élève se sente en confiance et puisse être pris en charge.

Certes la protection des mineurs est fondamentale, mais qu'en est-il des personnes âgées ? Celles-ci ne sont, dans certains cas, pas suffisamment habituées aux nouvelles technologies de l'information et de la communication. Les personnes d'un certain âge sont, parfois seules, et par conséquent, plus vulnérables. Tel pourrait être également le cas des personnes défavorisées ou présentant un déficit mental. Pourtant, certaines dispositions ne protègent que les mineurs comme par exemple celles concernant le *grooming* ou la cyberprédation. Il serait donc opportun d'élargir le champ d'application de ces dispositions afin qu'elles puissent être également applicables à d'autres situations de vulnérabilité et ainsi éviter des situations d'impunité.

Dans ce contexte, la preuve numérique revêt un caractère fondamental. Plusieurs dispositions pénales permettent, selon les cas, aux officiers de police judiciaire, au procureur du Roi ou au juge d'instruction de réaliser diverses méthodes d'enquête ainsi que de requérir la collaboration de différents acteurs. Ces mesures ont pour objet de récolter la preuve numérique et d'identifier l'auteur des comportements litigieux. La rapidité dans ce type d'affaires est primordiale afin d'éviter que des éléments de preuve ne disparaissent. Par conséquent, il devrait être permis à la police de s'adresser directement aux opérateurs et fournisseurs afin d'accéder aux données d'identification.

Sur de nombreuses plateformes, il est permis aux utilisateurs de signaler des propos ou des documents indésirables ou inappropriés. Il est important qu'une réaction instantanée

soit mise en place en vue de la suspension temporaire rapide du profil d'un utilisateur présumé harceleur ou de la suppression des documents et propos litigieux.

Finalement, de nombreuses méthodes de recherche sont limitées dans le temps. Il serait opportun d'augmenter la durée pendant laquelle ces mesures peuvent être effectuées afin de la faire correspondre à la pratique. En effet, la découverte des infractions prend souvent place un certain temps après la commission de celles-ci. Cela a pour conséquence, dans certains cas, de rendre inaccessibles les informations nécessaires aux autorités judiciaires.

Pour conclure, il est vrai que la législation belge s'adapte au fur et à mesure à cette nouvelle problématique sociétale. Mais elle doit, selon nous, poursuivre ses efforts d'adaptation en privilégiant une coopération rapide et efficace entre les différentes autorités judiciaires. Les techniques utilisées deviennent de plus en plus performantes ce qui exige une formation adaptée des autorités judiciaires.

Bibliographie

❖ Législation

➢ Législation internationale

Pacte international relatif aux droits civils et politiques, fait à New York le 19 décembre 1966, approuvé par la loi du 15 mai 1981, *M.B.*, 6 juillet 1983.

➢ Législation européenne

- Législation du 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 Conseil de l'Europe sur la cybercriminalité, signée à Budapest le 23 novembre 2001, *S.T.E.*, n° 185.

Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels, signée à Lanzarote le 25 octobre 2007, *S.T.C.E.*, n° 201.

- Législation de l'Union européenne

Charte des droits fondamentaux de l'Union européenne, adoptée à Nice le 7 décembre 2000.

Directive 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 (2002/58/CE), *J.O.C.E.*, L-201, 31 juillet 2002 (modifiée par la Directive du Parlement européen et du Conseil du 15 mars 2006 (2006/24/CE), *J.O.U.E.*, L-105, 13 avril 2006, mais abrogée depuis lors et par la Directive du Parlement européen et du Conseil du 25 novembre 2009 (2009/136/CE), *J.O.U.E.*, L-337, 18 décembre 2009).

Directive du Parlement européen et du Conseil 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 (2011/93/UE), *J.O.U.E.*, L-335/1, 17 décembre 2011.

Décision-cadre du Conseil du 28 novembre 2008 sur la lutte contre certaines formes et manifestations de racisme et de xénophobie au moyen du droit pénal (2008/913/JAI), *J.O.U.E.*, L-328/55, 6 décembre 2008.

Résolution du Parlement européen du 1er mars 2018 sur la situation des droits fondamentaux dans l'Union européenne en 2016 (2017/2125(INI)), *J.O.U.E.*, C/129/14, 5 avril 2019.

- Divers

Recommandation du Comité des ministres du 11 septembre 1995 aux États membres relative aux problèmes de procédure pénale liés à la technologie de l'information (R(95)13).

Communication de la Commission européenne du 26 janvier 2001 au Conseil, au Parlement, au Comité économique et social, au Comité des régions - Créer une société de l'information plus sûre en renforçant la sécurité des infrastructures de l'information et en luttant contre la cybercriminalité, COM (2000) 890.

CONSEIL DE L'EUROPE, « Rapport explicatif de la Convention sur la cybercriminalité », Budapest, 23 novembre 2001, disponible sur https://rm.coe.int/16800ccea4 (25 juin 2019).

EUROPEAN COMMISSION, « Code of conduct on countering illegal hate speech online », 31 mai 2016, disponible sur https://ec.europa.eu/info/sites/info/files/code_of_conduct_on_countering_illegal_hate_speech_online_en.pdf (3 juillet 2019).

➢ Législation belge

C.i.cr., art. 8, 28*bis*, 28*sexies*, 39*bis*, 39*ter*, 39*quater*, 46*bis*, 46*sexies*, 87, 88, 88*bis*, 88*ter*, 88*quater*, 88*sexies*, 90*ter*, 90*quater*, 90*novies* et 99*quater*.

Const., art. 19, 22 et 29.

C. pén., art. 65, 327, 337*ter*, 337*quater*, 371/1, 377, 377bis, 377*ter*, 377*quater*, 417*quinquies*, 433*bis*/1, 442*bis*, 443, 444, 448, 450 et 453*bis*.

C. jud., art. 119 et 259*sexies*.

Loi du 8 avril 1965 relative à la protection de la jeunesse, à la prise en charge des mineurs ayant commis un fait qualifié infraction et à la réparation du dommage causé par ce fait, *M.B.*, 15 avril 1965.

Loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques, *M.B.*, 21 mars 1991.

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

Loi du 30 octobre 1998 qui insère un article 442bis dans le Code pénal en vue d'incriminer le harcèlement, *M.B.*, 17 décembre 1998.

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

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

Loi du 25 avril 2007 portant des dispositions diverses (IV), *M.B.*, 8 mai 2007.

Loi du 26 novembre 2011 modifiant et complétant le Code pénal en vue d'incriminer l'abus de la situation de faiblesse des personnes et d'étendre la protection pénale des personnes vulnérables contre la maltraitance, *M.B.*, 23 janvier 2012.

Loi du 24 octobre 2013 modifiant le titre préliminaire du Code de procédure pénale en ce qui concerne les nullités, *M.B.*, 12 novembre 2013.

Loi du 10 avril 2014 modifiant le Code pénal en vue de protéger les enfants contre les cyberprédateurs, *M.B.*, 30 avril 2014.

Loi du 10 avril 2014 relative à la protection des mineurs contre la sollicitation à des fins de perpétration d'infractions à caractère sexuel, *M.B.*, 30 avril 2014.

Loi du 1er février 2016 modifiant diverses dispositions en ce qui concerne l'attentat à la pudeur et le voyeurisme, *M.B.*, 19 février 2016.

Loi du 26 mars 2016 modifiant l'article 442*bis* du Code pénal, *M.B.*, 5 avril 2016.

Loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques, *M.B.*, 18 juillet 2016.

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.

Loi du 5 mai 2019 portant des dispositions diverses en matière pénale et en matière de cultes, et modifiant la loi du 28 mai 2002 relative à l'euthanasie et le Code pénal social, *M.B.*, 24 mai 2019.

Projet de loi portant réforme de certaines entreprises publiques économiques, Exposé des motifs, *Doc. parl.*, Chambre, 1989-1990, n° 47-1287/1, 24 septembre 1990.

Proposition de loi insérant un article 460*ter* dans le Code pénal en vue d'incriminer le harcèlement, Amendement, *Doc. parl.*. Chambre, 1997-1998, n° 49-1046/6, 9 juin 1998.

Proposition de loi insérant un article 460*ter* dans le Code pénal en vue d'incriminer le harcèlement, *Doc. parl.*, Chambre, 1997-1998, n° 49-1046/8, 3 juillet 1998.

Projet de loi relatif à la criminalité informatique, Exposé des motifs, *Doc. parl.*, Chambre, 1999-2000, n° 50-213/1, 3 novembre 1999.

Proposition de loi visant à réprimer le *happy slapping*, *Doc. parl.*, Chambre, 2006-2007, n° 51-3079/1, 13 avril 2007.

Proposition de loi visant à réprimer le *happy slapping*, *Doc. parl.*, Chambre, 2007-2008, n° 52-497/1, 4 décembre 2007.

Proposition de loi visant à réprimer le *happy slapping*, *Doc. parl.*, Chambre, 2010-2011, n° 53-417/1, 19 octobre 2010.

Proposition de loi modifiant le Code pénal en vue de garantir la protection pénale des enfants contre le « *grooming* » (mise en confiance à des fins d'abus sexuel), *Doc. parl.*, Sénat, 2013-2014, n° 5-1823/4, 26 février 2014.

Proposition de loi modifiant le Code pénal en vue de protéger les enfants contre les cyberprédateurs, Discussion des articles, *Doc. parl.*, Sénat, 2013-2014, n° 5-2253/3, 26 février 2014.

Projet de loi modifiant le Code pénal en vue de protéger les enfants contre les cyberprédateurs, Discussion des articles et votes, *Doc. parl.*, Chambre, 2013-2014, n° 53-3450/2, 24 mars 2014.

Proposition de loi modifiant le Code pénal en ce qui concerne l'incrimination de l'attentat à la pudeur, *Doc. parl.*, Chambre, 2014-2015, n° 54-699/1, 10 décembre 2014.

Proposition de loi modifiant le Code pénal en ce qui concerne l'incrimination de l'attentat à la pudeur, Amendement, *Doc. parl.*, Chambre, 2014-2015, n° 54-699/2, 15 juillet 2015.

Proposition de loi modifiant le Code pénal en ce qui concerne l'incrimination de l'attentat à la pudeur, Amendement, *Doc. parl.*, Chambre, 2015-2016, n° 54-699/3, 27 novembre 2015.

Projet de loi relatif à la collecte et à la conservation des données dans le secteur des communications électroniques, Exposé des motifs, *Doc. parl.*, Chambre, 2015-2016, n° 54-1567/1, 11 janvier 2016.

Proposition de loi modifiant le Code pénal en ce qui concerne l'incrimination du harcèlement moral, Discussion des articles et votes, *Doc. parl.*, Chambre, 2015-2016, n° 54-463/3, 2 mars 2016.

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.*, Chambre, 2015-2016, n° 54-1966/1, 8 juillet 2016.

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, Avis de la Commission vie privée, *Doc. parl.*, Chambre, 2015-2016, n° 54-1966/2, 11 juillet 2016.

➢ Législation française

C. pén., art. 222-33-3 et 223-13.

❖ Jurisprudence

➢ Jurisprudence de la Cour européenne des droits de l'homme

Cour eur. D.H., arrêt Funke c. France, 25 février 1993, req. n° 110588/83.

Cour eur. D.H., arrêt Saunders c. Royaume-Uni, 17 décembre 1996, req. n° 1187/91.

Cour eur. D.H., arrêt Jalloh c. Allemagne, 11 juillet 2006, req. n° 54810/00.

Cour eur. D.H., arrêt Maschino c. France, 16 octobre 2008, req. n° 10447/03.

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

Cour eur. D.H., arrêt Brusco c. France, 14 octobre 2010, req. n° 1466/07.

Cour eur. D.H., arrêt Vinci construction et GMT Génie Civil et services c. France, 2 avril 2014, req. n° 63629/10.

Cour eur. D.H., arrêt Trabajo Rueda c. Espagne, 30 mai 2017, req. n° 32600/12.

- Jurisprudence belge

C.A., 10 mai 2006, n° 71/2006.

C.A., 14 juin 2006, n° 98/2006.

C.A., 28 mars 2007, n° 55/2007.

C.A., 18 avril 2007, n° 64/2007.

C.C., 10 mai 2007, n° 75/2007.

C.C., 5 mai 2009, n° 76/2009.

C.C., 22 décembre 2011, n° 198/2011, note F. Vandevenne, *Rev. Dr. Pén. Crim.,* 2012/7-8, p. 810.

C.C., 6 décembre 2018, n° 174/2018.

Cass. (2e ch.), 26 mars 2003, *J.T.*, 2003, p. 626.

Cass. (2e ch.), 14 octobre 2003, R.G. n° P.03.0762.N.

Cass. (2e ch.), 21 février 2007, *J.T.*, 2007, p. 262.

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

Cass. (2e ch.), 6 mars 2012, R.G. n° P.11.0855.N, *N.J.W*, 2012/9, n° 262, p. 341.

Cass. (2e ch.), 6 mars 2012, R.G. n° P.11.1374.N.

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

Cass. (2e ch.), 20 février 2013, R.G. n° P.12.1629.F.

Cass. (2e ch.), 29 octobre 2013, R.G. n° P.13.1270.N.

Cass. (2e ch.), 27 novembre 2013, R.G. n° P.13.0714.F.

Cass. (2e ch.), 11 février 2015, R.G. n° P.14.1739.F.

Cass. (2e ch.), 31 mars 2015, R.G. n° P.14.0293.N.

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

Cass. (2e ch.), 8 novembre 2016, R.G. n° P.16.0958.N.

Cass. (2e ch.), 28 mars 2017, R.G. n° P.16.1245.N.

Cass. (2e ch.), 19 février 2019, R.G. n° P.17.1229.N.

Bruxelles (11e ch.), 27 juin 2000, *A.M.*, 2001/1, p. 142.

Bruxelles (13e ch.), 4 avril 2007, *A&M*, 2009/1-2, p. 172.

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

Bruxelles (13e ch.), 12 octobre 2011, *A&M*, 2012/2-3, p. 238.

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

Gand, 23 juin 2015, *N.J.W.*, 2016/3, n° 336, p. 134, note C. Conings.

Anvers (4e ch.), 15 novembre 2017, inédit, R.G. n° C.1288.2017.

Anvers (mis. acc.), 21 décembre 2017, inédit, R.G. n° K.2895.2017.

Corr. Bruxelles, 22 décembre 1999, *A.M.*, 2000, p. 134.

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

Corr. Anvers (div. Turnhout), 16 mai 2012, *T. Strafr.*, 2012/6, p. 474, note F.S.

Corr. Flandre orientale (div. Termonde), 17 novembre 2014, *T. Strafr.*, 2016/3, p. 255.

Corr. Flandre occidentale (div. Bruges), 19 avril 2016, *T.G.R.*, 2016, p. 300.

Corr. Anvers (div. Malines), 27 octobre 2016, *N.J.W.*, 2016/20, p. 921.

Corr. Anvers (div. Anvers), 24 avril 2018, *N.J.W*, 2018, p. 649, note S. Royer.

Corr. Liège (div. Liège), 7 septembre 2018, *J.L.M.B.*, 2018/38, p. 1817, note Q. Pironnet.

❖ Doctrine

BANNEUX, N. et KERZMANN, L., « Le mal nommé "harcèlement téléphonique" : chronique des tribulations législatives d'une infraction moderne », *R.D.T.I.*, 2009/1, n° 34, pp. 29 à 45.

BEAUDUIN, B. et DASNOY, N., « Relations professeurs/élèves : la ligne rouge : the case of cyberstalking », *New Journal of European Criminal Law*, 2012, n° 3(2), pp. 1 à 4.

BEERNAERT, M.-A, BOSLY, H.-D. et VANDERMEERSCH, D., *Droit de la procédure pénale*, 8e éd, tome I, Brugge, La Charte, 2017.

BEERNAERT, M.-A., COLETTE-BASECQZ, N., GUILLAIN, C., KENNES, L., MANDOUX, P., PREUMONT, M. et VANDERMEERSCH, D., *Introduction à la procédure pénale*, 6e éd., Bruxelles, La Charte, 2017.

BELLON, J.-P. et GARDETTE, B., *Harcèlement et cyberharcèlement à l'école – une souffrance scolaire 2.0*, Collection Pédagogies, Issy-les-Moulineaux, ESF, 2013.

BELSEY, B., « Cyberbullying : An emerging threat to the "always on" generation », 24 mars 2019, disponible sur http://www.billbelsey.com/?cat=13 (26 juillet 2019).

BLAYA, C., « *School bullying* : un type de victimisation en milieu scolaire. Définition et conséquences », *Victimes : du traumatisme à la restauration. Œuvre de justice et victimes*, sous la direction de R. Cario, vol. 2, Paris, L'Harmattan, 2002, pp. 125 à 142.

BLAYA, C., *Les ados dans le cyberspace : prises de risque et cyberviolence*, Bruxelles, De Boeck Supérieur, 2013.

BOSLY, H., DELHAISE, E., VANDERMEERSCH, D., COLETTE-BASECQZ, N., DE NAUW, A., MANDOUX, P. et NEDERLANDT, O., « Chronique semestrielle de jurisprudence », *Rev. dr. pén.*, 2019/5, pp. 569 à 683.

BRUN, M., « Lutte contre les discours haineux : le nouveau code de conduite de la Commission », 4 juin 2016, *EU-Logos Athéna*, disponible sur https://www.eu-logos.org/2016/06/04/lutte-contre-les-discours-haineux-le-nouveau-code-de-conduite-de-la-commission/ (3 juillet 2019).

CARBONNIER, J., *Sociologie juridique*, Paris, PUF, 1978.

CARNEROLI, S., « Note sous Corr. Liège (16e ch.), 7 septembre 2018 », *A&M*, 2018-2019/1, pp. 167 à 171.

COLETTE-BASECQZ, N., « La protection pénale des personnes vulnérables dans l'environnement numérique », *Vulnérabilités et droits dans l'environnement numérique*, Bruxelles, Larcier, 2018, pp. 133 à 177.

COLETTE-BASECQZ, N., « La responsabilité pénale liée au phénomène du cyberharcèlement et à ses différentes formes d'expression », *Responsabilités et numérique*, Limal, Anthemis, 2018, pp. 35 à 61.

DE HERT, P., MILLEN, J. et GROENEN, A., « Het delict belanging in wetgeving en rechtspraak. Bijna tot redelijke proporties gebracht », *T. Strafr.*, 2008/1, pp. 3 à 9.

DE NAUW, A. et KUTY, F., *Manuel de droit pénal spécial*, 4e éd., Liège, Wolters Kluwer, 2018.

DE RUE, M., « Le harcèlement », *Les infractions*, vol. 2 : Les infractions contre les personnes, Bruxelles, Larcier, 2010, pp. 725 à 745.

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

DE SCHRIJVER, V. et MISONNE, A., « Vie du droit. Un nouvel avatar de la législation par référence : la suppression de l'article 114, § 8, de la loi Belgacom », *J.T.*, 2005/34, n° 6196, pp. 637 à 639.

DE VALKENEER, C., *Manuel de l'enquête pénale*, 4e éd., Bruxelles, Larcier, 2011.

DECHAMPS, F. et LAMBILOT, C., « Cybercriminalité : état de la question », *B.S.J.*, 2016/559, pp. 7 à 10.

DECHAMPS, F. et LAMBILOT, C., *Cybercriminalité : état des lieux*, Limal, Anthemis, 2016.

DELHAISE, E., « Le suicide de Madison : enfin une prise de conscience en matière de harcèlement ? », 22 avril 2016, *Justice en ligne*, disponible sur http://www.justice-en-ligne.be/article861.html (1er août 2019).

EL ASAM, A. et SAMARA, M., « Cyberbullying and the law : A review of psychological and legal challenges », *Computers in human behavior*, vol. 65, Pergamon, 2016, pp. 127 à 141.

FORGET, C. et DUMORTIER, F., « Criminalité informatique », *R.D.T.I.,* 2015/2-3, n° 59-60, pp. 114 à 126.

FORGET, C., « La collecte de preuves informatiques en matière pénale », *Pas de droit sans technologie*, sous la direction de J.-F. Henrotte et F. Jongen, vol. 158, CUP, Bruxelles, Larcier, 2015, pp. 251 à 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 à 52.

FORGET, C., « Méthodes d'enquête pénales et protection des personnes vulnérables dans l'environnement numérique », *Vulnérabilités et droits dans l'environnement numérique*, Bruxelles, Larcier, 2018, pp. 179 à 203.

FRANSSEN, V. et TOSZA, S., « Vers plus de droits pour le justiciable sur internet ? Un nouveau cadre légal pour lutter contre la criminalité dans la société de l'information », *Les droits des justiciables face à la justice pénale*, Limal, Anthemis, 2017, pp. 205 à 249.

GIACOMETTI, M. et MONVILLE, P., « Réseaux sociaux, anonymat et faux profils : vrais problèmes en droit pénal et de la procédure pénale », *Les réseaux sociaux et le droit*, sous la direction de M. Salmon, Bruxelles, Larcier, 2014, pp. 179 à 210.

GOSSÉ, A., « Dans quelle mesure les autorités judiciaires belges peuvent-elles contraindre des entreprises de télécommunication étrangères à collaborer à une enquête pénale en Belgique ? », *Rev. dr. pén. entr.*, 2017/3, pp. 179 à 204.

GRIGG, D.K., « Cyber-agression : definition and concept of cyberbullying », *Australian Journal of Guidance and Counselling*, 2010, n° 20.

GUILLOUX, R., *Situations de harcèlement entre élèves. Comprendre & aider*, 2018, *Retz*, disponible sur http://extranet.editis.com/it-yonixweb/images/322/art/doc/8/8d9faf212331353135373531363839323935 31.pdf (26 juillet 2019).

HENRION, T., « Écoutes téléphoniques », X., *Postal Mémorialis – Lexique du droit pénal et des lois spéciales*, Malines, Kluwer, 2009, pp. E43/01 à E43/65.

HUMBEECK, B., LAHAYE, W. et BERGER, M., *Prévention du harcèlement et des violences scolaires. Prévenir, agir, réagir…*, Louvain-la-Neuve, De Boeck, 2016.

ISGOUR, M., « La protection juridique de l'e-réputation des personnes physiques et morales », *L'élément moral en droit. Une vision transversale*, sous la direction de F. Lambinet, Limal, Anthemis, 2014, pp. 93 à 145.

JONGEN, F. et STROWEL, A., « Droit à l'honneur et à la réputation », *Droit des médias et de la communication*, Bruxelles, Larcier, 2017, pp. 445 à 475.

JOUROVÁ, V., « *Code of Conduct on countering illegal hate speech online: First results on implementation* », décembre 2016, disponible sur http://ec.europa.eu/information_society/newsroom/image/document/2016-50/factsheet-code-conduct-8_40573.pdf (6 juillet 2019).

JOUROVÁ, V., « *Code of Conduct on countering illegal hate speech online – Results of the fourth monitoring exercise* », février 2019, disponible sur https://ec.europa.eu/info/sites/info/files/code_of_conduct_factsheet_7_web.pdf (6 juillet 2019).

KAUFMAN, G.A., *Liberté d'expression et protection des groupes vulnérables sur Internet*, Paris, L'Harmattan, 2016.

KERKHOFS, J. et VAN LINTHOUT, P., « Artikel 46*bis* van het Wetboek van strafvordering en de motiveringsplicht: de minimis non curat praetor », *T. Strafr.*, 2011/6, pp. 426 à 431.

KERKHOFS, J. et VAN LINTHOUT, P., « Cybercriminaliteit doorgelicht », *T. Strafr.*, 2010/4, pp. 179 à 199.

KERZMANN, L., « L'affaire Yahoo! Ou à qui s'adresse l'obligation de collaboration instaurée par l'article 46*bis* du Code d'instruction criminelle ? », *R.D.T.I.*, n° 44, 2011, pp. 116 à 123.

KUTY, F., « La minorité pénale », *Principes généraux du droit pénal belge*, Bruxelles, Larcier, 2010, pp. 387 à 415.

KUTY, F., « Le concours idéal d'infractions par unité d'intention ou de réalisation », *Principes généraux du droit pénal belge*, tome IV : La peine, Bruxelles, Larcier, 2017, pp. 930 à 987.

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 à 843.

LEROUX, O., « Criminalité informatique », X., *Postal Mémorialis - Lexique du droit pénal et des lois spéciales*, Waterloo, Kluwer, 2014, pp. C362/01 à C362/55.

LEROUX, O., « Criminalité informatique aspécifique », *Les infractions,* 2e éd.*,* vol. 1 : Les infractions contre les biens, Bruxelles, Larcier, 2016, pp. 509 à 534.

Leroux, O., « Criminalité informatique spécifique », *Les infractions,* 2e éd., vol. 1 : Les infractions contre les biens , Bruxelles, Larcier, 2016, pp. 448 à 508.

M. TÖLLER, « Revenge porn ou vengeance pornographique », *R.D.T.I.*, 2018/2, n° 71, pp. 87 à 105.

MASSART, G., « Régularité de la preuve: un cadre légal pour la jurisprudence Antigone », 16 décembre 2013, *Elegis*, disponible sur http://www.elegis.be/fr/nouvelle/regularite-de-la-preuve-un-cadre-legal-pour-la-jurisprudence-antigone (27 mars 2019).

MASSET, A. et BASTIAEN, V., « La séparation de fait et quelques infractions pénales spécifiques : le harcèlement entre époux », *Séparation de fait. Commentaires pratiques*, Waterloo, Kluwer, 2004.

MICHIELS, O. et FALQUE, G., « Les actes d'enquête », *Principes de procédure pénale*, Bruxelles, Larcier, 2019, pp. 141 à 208.

NEDERLANDT, O. et VANSILIETTE, F., « Droit pénal spécial – Les infractions du Code pénal », *Chronique de droit pénal*, Bruxelles, Larcier, 2017, pp. 164 à 294.

NIHOUL, N. et WATTIER, S., « La protection de la personne en situation de vulnérabilité par le droit des libertés publiques dans l'environnement numérique », *Vulnérabilités et droits dans l'environnement numérique*, Bruxelles, Larcier, 2018, pp. 9 à 29.

OLWEUS, D., *Violences entre élèves, harcèlements et brutalités : Les faits, les solutions*, Collection Pédagogies, Issy-les-Moulineaux, ESF, 1999.

PIRONNET, Q., « Des insultes sur les réseaux sociaux ne relèvent pas du délit de presse », *J.L.M.B.*, 2018/38, pp. 1825 à 1831.

ROEX, R., « Belgische justitie kan rechtstreeks informatie opvragen van Amerikaanse techreuzen », *Juristenkrant*, 2015, n° 319, p. 5.

ROEX, R., « De Yahoo-zaak: Belgische justitie plant vlag in cyberspace », *Vigiles*, 2016/2, pp. 69 à 73.

ROSIER, K., « Le spamming politique : affaire de harcèlement, de prospection et de traitement de données à caractère personnel ? », *Rev. dr. pén. entr.*, 2010/4, pp. 321 à 330.

VAN CLEEMPUT, K., LIEVENS, E. et PABIAN, S., « Een empirisch en juridisch perspectief op cyberpesten: naar een holistische aanpak », *T.J.K.*, 2016/1, pp. 6 à 22.

VAN ENIS, Q., « Entre interprétation restrictive du délit de presse et interprétation extensive de l'infraction de harcèlement : un régime en clair-obscur pour la vidéo en ligne ? », *J.T.*, 2014/21, n° 6565, pp. 393 à 397.

VAN ENIS, Q., « La Cour de cassation admet que l'on puisse se rendre coupable d'un délit de presse sur l'internet. Le temps du "délit de presse 2.0" est-il (enfin) arrivé ? », *J.T.*, 2012/23, n° 6483, pp. 505 à 507.

VANDEBOSCH, H. et VAN CLEEMPUT, K., « Defining cyberbullying: A qualitative research into the perceptions of youngsters », *CyberPsychology & Behavior*, vol. 11, Mary Ann Liebert, 2008, n° 4, disponible sur https://pdfs.semanticscholar.org/ee17/16f4ebdef031b324262335625a15d9c9f34b.pdf (27 juillet 2019).

VANDERMEERSCH, D., « Les recherches en matière de téléphonie mobile et de (télé)communications », *Colloque en droit pénal et procédure pénale*, sous la présidence de D. Bosquet, Bruxelles, Jeune barreau de Bruxelles, 2006, pp. 29 à 64.

VANDEVENNE, F., « Note : le harcèlement de retour à la Cour constitutionnelle », *Rev. Dr. Pén. Crim.,* 2012/7-8, pp. 814 à 820.

VILLÉE, C., WINTGENS, K. et GÉRARD, S., « De quelques précautions à l'usage d'Internet », *JDJ*, 2009/6, n° 286, pp. 42 à 45.

WALRAVE, M., DEMOULIN, M., HEIRMAN, W. et VAN DER PERRE, A., *Cyberharcèlement : risque du virtuel, impact dans le réel*, Bruxelles, Observatoire des Droits de l'Internet, 2009.

WARTEL, N., MARHRAOUI, O. et DE SALLE, C., « Le cyber-harcèlement des enfants & des adolescents », 2017, *Les études du Centre Jean Gol*, disponible sur http://www.cjg.be/wp-content/uploads/2017/03/CJG_ETUDE_Cyber_Harcelement.pdf (25 juillet 2019).

WILLARD, N., « Cyberbullying legislation and school policies: Where are the boundaries of the "schoolhouse gate" in the new virtual world? », mars 2007, disponible sur http://www.embracecivility.org/wp-content/uploadsnew/2012/10/cblegislation.pdf (26 juillet 2019).

❖ Divers

➢ Sites Web

FAURE, L., « Google+ : Fermeture officielle du réseau social de Google », 3 avril 2019, *IT Social*, disponible sur https://itsocial.fr/actualites/google-annonce-officiellement-processus-de-fermeture-de-google/ (7 juillet 2019).

Le téléphone de Louise, une initiative réalisée par *VOO* en partenariat avec la Police Fédérale, disponible sur https://www.letelephonedelouise.com (2 octobre 2018).

X., « Federal Computer Crime Unit », 2019, *Police Fédérale*, disponible sur https://www.police.be/5998/fr/a-propos/directions-centrales/federal-computer-crime-unit (28 juillet 2019).

X., « La police fédérale présente le Moniteur de sécurité 2018 », 3 juillet 2019, *Police Fédérale*, disponible sur https://www.police.be/5998/fr/actualites/la-police-federale-presente-le-moniteur-de-securite-2018 (27 juillet 2019).

X., « Moniteur de sécurité 2018 : Grandes tendances », 3 juillet 2019, *Police Fédérale*, disponible sur http://www.moniteurdesecurite.policefederale.be/assets/pdf/2018/reports/Grandes_tendances_Analyses_VMS2018.pdf (27 juillet 2019).

➢ Articles de presse

ENGLER, S., « La Federal Computer Crime Unit manque de personnel », 30 avril 2018, *RTBF*, disponible sur https://www.rtbf.be/info/belgique/detail_la-federal-computer-crime-unit-manque-de-personnel?id=9906286 (2 août 2019).

HOVINE, A., « Cyber-harcèlement : Un quart des jeunes ont déjà été insultés sur internet », 14 avril 2016, *La Libre*, disponible sur https://www.lalibre.be/belgique/cyber-harcelement-un-quart-des-jeunes-ont-deja-ete-insultes-sur-internet-570e717335702a22d65948eb (28 juillet 2019).

KUDRYAVTSEV, K., « Que fait l'Union européenne contre le cyberharcèlement ? », 20 février 2019, *FranceSoir*, disponible sur http://www.francesoir.fr/politique-monde/que-fait-union-europeenne-contre-le-cyberharcelement (5 juillet 2019).

WAUTERS, L., « "Injurier n'est pas exprimer une opinion" : prison ferme pour des propos sur Facebook », 28 mai 2019, *Le Soir+*, disponible sur https://plus.lesoir.be/227594/article/2019-05-28/injurier-nest-pas-exprimer-une-opinion-prison-ferme-pour-des-propos-sur-facebook (31 juillet 2019).

X., « Haine sur internet : Jeuxvideo.com va se plier au code de conduite de l'UE », 4 février 2019, *RTL Info*, disponible sur https://www.rtl.be/info/magazine/hi-tech/haine-sur-internet-jeuxvideo-com-va-se-plier-au-code-de-conduite-de-l-ue-1097504.aspx (5 juillet 2019).

ANNEXE 1 : Analyse du code de conduite du 31 mai 2016 de la Commission européenne visant à combattre les discours de haine illégaux en ligne – Résultats de la quatrième évaluation de février 2019

Source : V. JOUROVÁ, « Code of Conduct on countering illegal hate speech online – Results of the fourth monitoring exercise », février 2019, pp. 2 à 5, disponible sur https://ec.europa.eu/info/sites/info/files/code_of_conduct_factsheet_7_web.pdf (6 juillet 2019).

Tableau 1:

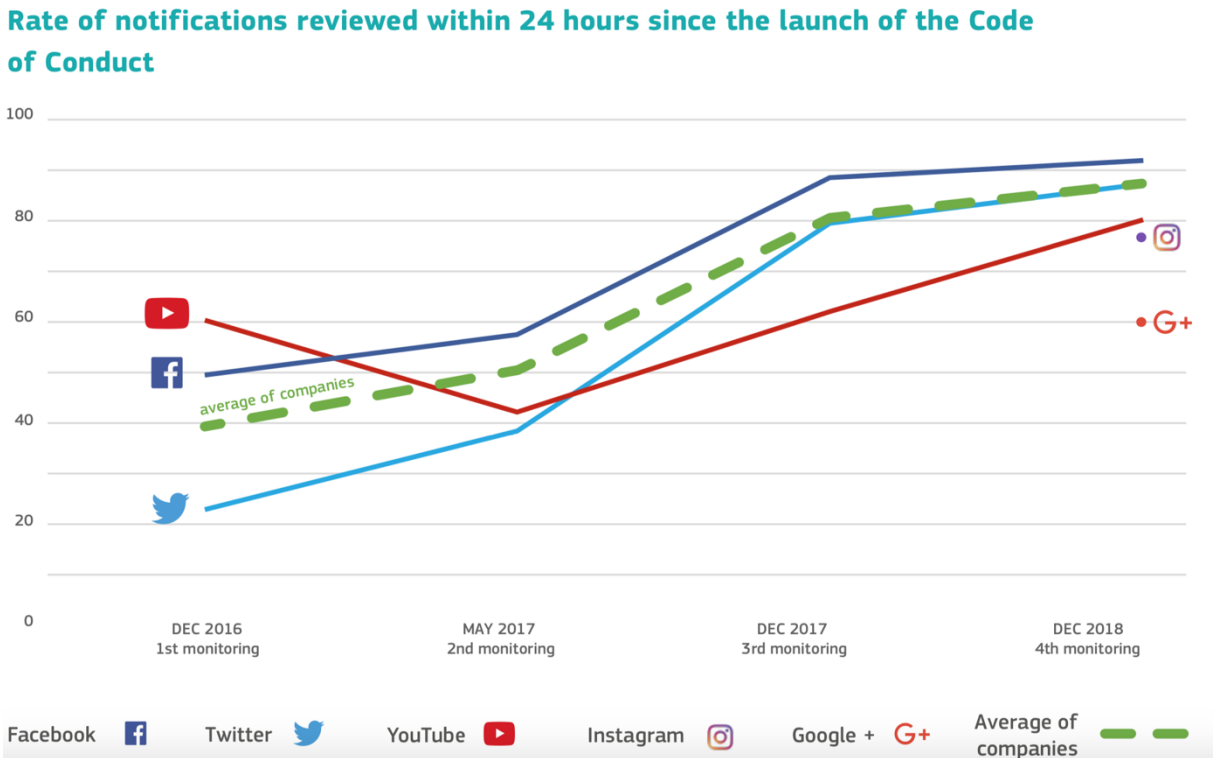


Tableau 2:

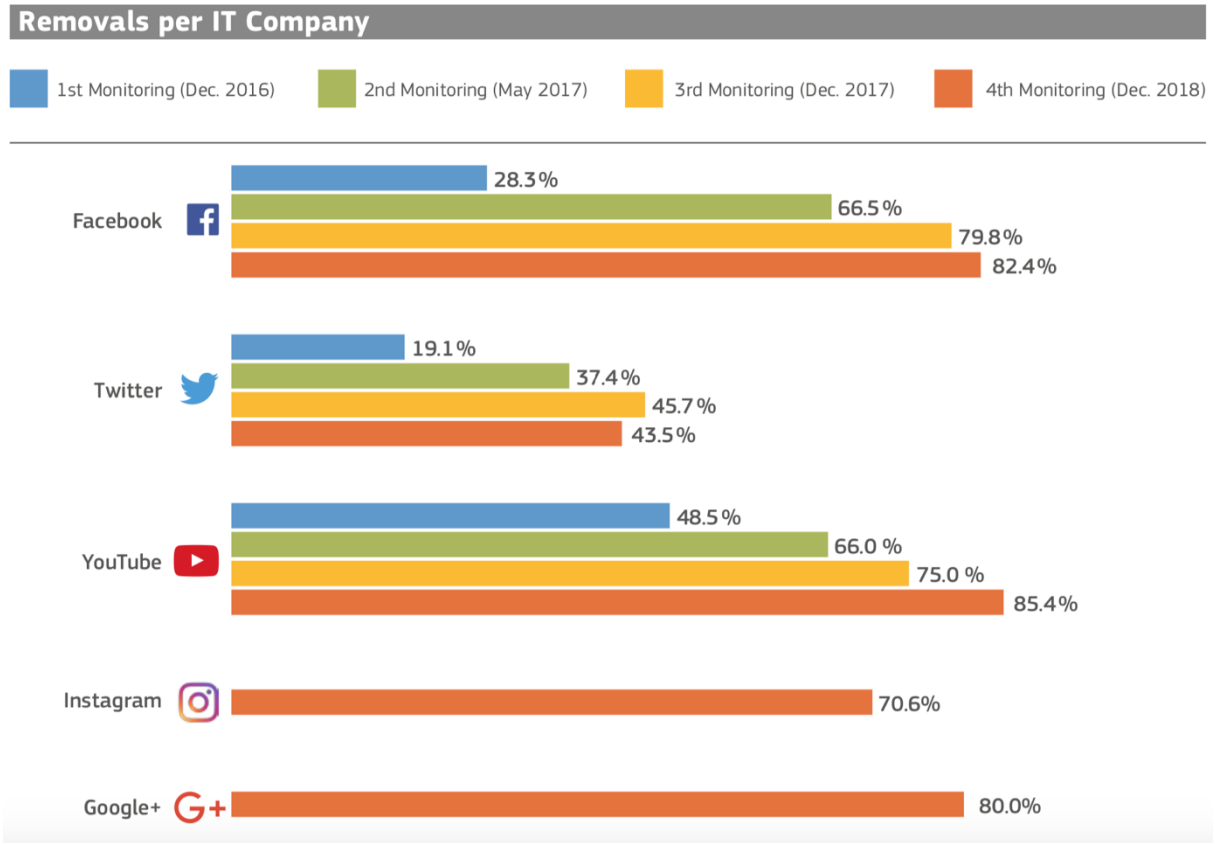
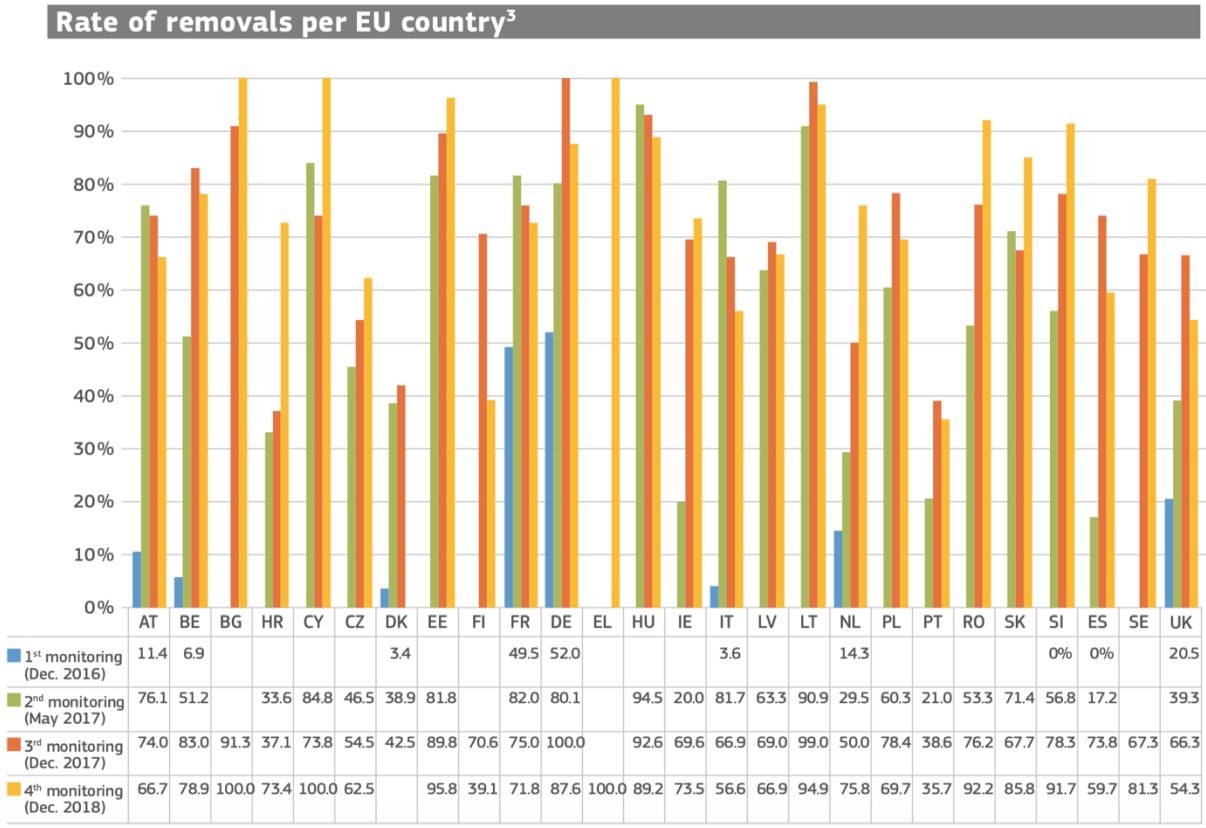

Removals per IT Company
1st Monitoring (Dec. 2016)
2nd Monitoring (May 2017)
3rd Monitoring (Dec. 2017)
4th Monitoring (Dec. 2018)
Facebook
28.3%
66.5%
79.8%
82.4%
Twitter
19.1%
37.4%
45.7%
43.5%
YouTube
48.5%
66.0 %
75.0 %
85.4%
Instagram
70.6%
Google+
80.0%

Tableau 3:



	AT	BE	BG	HR	CY	CZ	DK	EE	FI	FR	DE	EL	HU	IE	IT	LV	LT	NL	PL	PT	RO	SK	SI	ES	SE	UK
1st monitoring (Dec. 2016)	11.4	6.9					3.4			49.5	52.0				3.6			14.3					0%	0%		20.5
2nd monitoring (May 2017)	76.1	51.2		33.6	84.8	46.5	38.9	81.8		82.0	80.1		94.5	20.0	81.7	63.3	90.9	29.5	60.3	21.0	53.3	71.4	56.8	17.2		39.3
3rd monitoring (Dec. 2017)	74.0	83.0	91.3	37.1	73.8	54.5	42.5	89.8	70.6	75.0	100.0		92.6	69.6	66.9	69.0	99.0	50.0	78.4	38.6	76.2	67.7	78.3	73.8	67.3	66.3
4th monitoring (Dec. 2018)	66.7	78.9	100.0	73.4	100.0	62.5		95.8	39.1	71.8	87.6	100.0	89.2	73.5	56.6	66.9	94.9	75.8	69.7	35.7	92.2	85.8	91.7	59.7	81.3	54.3

À propos des tableaux 2 et 3 :

Marine Fanourakis 7 juillet 2019 à 15:12

Code of Conduct on countering illegal hate speech online – Results of the fourth monitoring

À : vera-jourova-contact@ec.europa.eu

Dear Madam Jourova,

I am studying law and writing my thesis on cyber bullying. I found this document which is very interesting:
https://ec.europa.eu/info/sites/info/files/code_of_conduct_factsheet_7_web.pdf

I tried to understand the results from the tables « Removals per IT company » (p.3) and « Rate of removals per EU country » (p.4).

I am not sure to understand well the interpretation to give to these two tables.

1. Should I understand it like: companies and countries are delating less because there are less speeches considered as illegal?

2. Should I understand it like: companies and countries are delating less because they are less reactive?

Best regards,

Marine Fanourakis

JUST-NO-HATE@ec.europa.eu 15 juillet 2019 à 09:45

RE: Code of Conduct on countering illegal hate speech online – Results of the fourth monitoring Détails

À : marinefanourakis@gmail.com, Cc : JUST-C2@ec.europa.eu

Dear Ms Fanourakis,

Many thanks for your email of 7 July 2019 addressed to the Commissioner for Justice and Consumers, Ms Věra Jourová. In your email, you are asking some questions in relation to the 4th monitoring exercise on the implementation of the Code of conduct on countering illegal content online.

Since the monitoring of the Code of conduct is under the responsibility of this Unit, we are replying on behalf of Commissioner Jourová.

Regarding your questions, each monitoring exercise is based on a sample of notifications sent to IT Companies by a network of civil society organisations or public bodies from the different Member States. It is however not a representative sample and it does not allow to draw any conclusion on the amount of illegal hate speech in specific countries or companies. By using a standardised methodology, the monitoring exercise enables to establish general trends over time on the reaction by IT Companies to hate speech notifications (in particular removal rate and time of assessment). It must be noted also that, while globally the number of notifications is sufficiently high to provide reliable trends, when it comes to country level breakdown these numbers may be too limited to draw specific conclusions on the effectiveness of the companies' reaction in each national context.

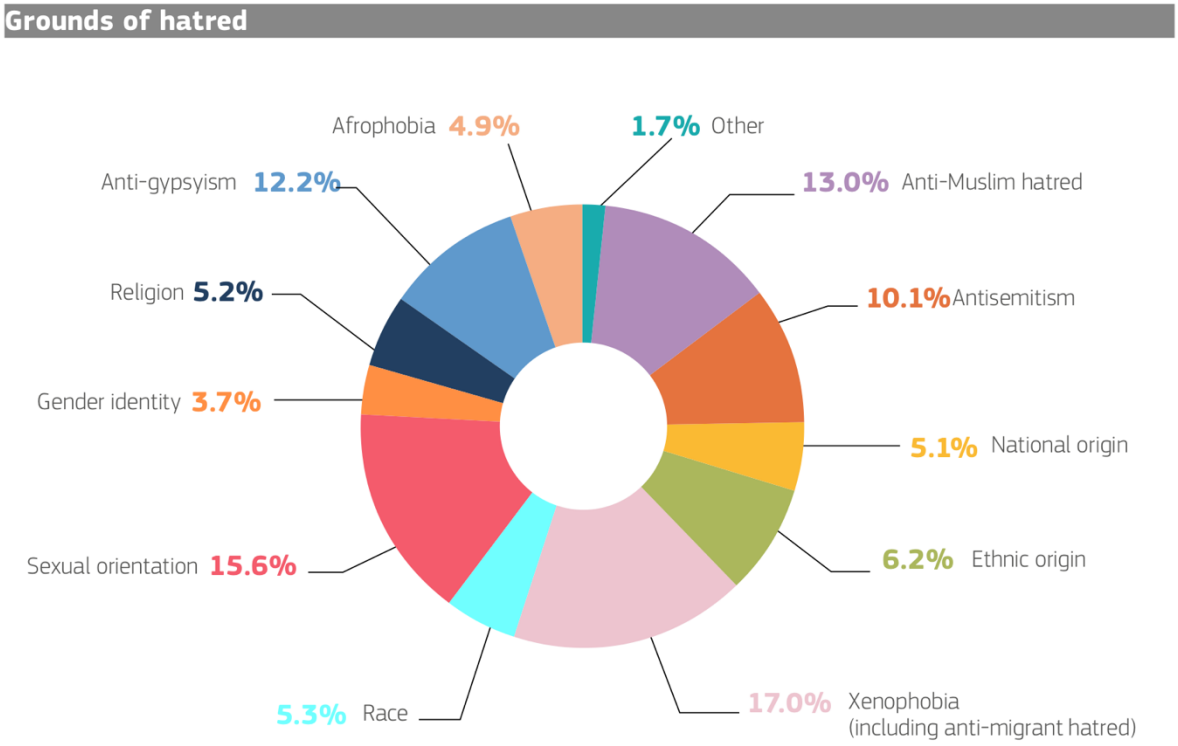
This is further explained in a footnote to the graph at page 4 of the factsheet as well as in the methodology part at page 6.
For more information on the Code of conduct and the monitoring exercise, please consult the Q&A at the following link:
http://europa.eu/rapid/press-release_MEMO-19-806_en.htm

We hope you will find the reply useful, and please do not hesitate to reach out to us in case of further queries.

Kind regards,

The JUST NO HATE Team

Tableau 4:


Grounds of hatred
Afrophobia 4.9%
1.7% Other
Anti-gypsyism 12.2%
13.0% Anti-Muslim hatred
Religion 5.2%
10.1% Antisemitism
Gender identity 3.7%
5.1% National origin
Sexual orientation 15.6%
6.2% Ethnic origin
5.3% Race
17.0% Xenophobia
(including anti-migrant hatred)

ANNEXE 2 : Interview du 4 juillet 2019 avec Olivier Bogaert (Commissaire à la Computer Crime Unit de la Police Fédérale)

Les enfants/adolescents peuvent-ils être considérés comme des personnes vulnérables ?

L'adolescence est une phase de fragilité qui peut être mise en évidence, car il existe une impulsivité liée aux modifications corporelles.
Bruno Humbeeck s'intéresse à cette problématique et met en évidence qu'il y a chez les enfants et les adolescents des phases qui vont faciliter les phénomènes de harcèlement et qui vont pouvoir se développer avec le numérique. À la rentrée scolaire, les groupes se structurent et les leaders vont assurer leur autorité sur le groupe. On a ensuite la phase des vacances avec les fêtes de fin d'année apaisant la situation. À la rentrée le leader doit à nouveau, assurer son autorité. À ce moment-là, il peut cibler un certain nombre de personnes/ membres de la classe. Cela peut s'appuyer sur l'aspect physique ou sur des fragilités comme par exemple des problèmes d'expression. Selon Bruno Humbeeck, il y a une phase de harcèlement extrêmement intense liée à la thématique hormonale. Cette phase est d'autant plus intense quand le printemps arrive durant les mois de mars, avril et mai. On assiste à une retombée par après lors de la période d'examens.

Quel est le lien existant entre l'article 145, paragraphe 3*bis*, de la loi de 2005 et les dispositions du Code pénal (ex : calomnie, diffamation, etc.) ? Est-ce que l'ensemble de ces infractions peuvent être considérées comme du cyber-harcèlement ?

Le cyber-harcèlement n'existe pas en tant que tel. Le policier pourra jouer la carte de la calomnie et de la diffamation. Puis, le magistrat pourra éventuellement décider d'une autre approche en fonction des éléments dont il aura eu connaissance.

L'article 145, paragraphe 3*bis* loi de 2005 sur les communications est souvent retenu par les magistrats, car la peine peut aller jusqu'à 2 ans de prison, ce qui est conséquent. Cette infraction peut venir s'ajouter à d'autres infractions du Code pénal (ex : insultes, moqueries, diffusion d'images, etc.).

Qu'est-ce qu'il en est de la preuve numérique ?

Il est préférable que la victime se présente avec un dossier déjà relativement complet. Il est nécessaire d'avoir un maximum de captures d'écran permettant de comprendre le délai qui s'est écoulé depuis que la victime subit les faits et ainsi voir les différents contenus. C'est ce qu'on appelle une preuve numérique.

À partir de septembre 2019, un outil développé par l'Université de Mons, avec l'appui de la Ville de Mons, sera mis à disposition des écoles. Il s'agit d'un projet pédagogique s'inscrivant dans la gestion du harcèlement et cyber-harcèlement dans les écoles. Cet outil consiste en une application appelée « Cyber Help » et qui est déjà disponible dans les stores de Apple et Google. Pour la faire fonctionner, il faut disposer d'un code que l'école va fournir. L'élève victime, une fois l'application installée, va voir apparaitre sur l'écran un petit personnage. En cliquant dessus une capture du contenu sera automatiquement créée. Cette capture sera envoyée à l'adresse e-mail de l'école. L'école recevra le message généré à partir du téléphone de l'élève. L'école va voir les contenus et aura l'ensemble des éléments afin de comprendre ce que la victime vit. Elle pourra ainsi prendre l'élève en charge. Au niveau de la procédure, ce projet apporte un élément intéressant. L'application pourra fournir un dossier complet aux policiers étant amenés à intervenir dans le dossier. Elle n'est pas encore active, car c'est à l'école de l'activer. L'école doit lancer le processus, doit désigner des éducateurs prenant en charge le mécanisme, etc.

Qu'est-ce que les Federal et Regional Computer Crime Units ? Existe-t-il d'autres unités spécialisées dans le cyber-harcèlement ?

L' « Unité I2 » fait la veille sur internet, elle bloque les plateformes à problèmes. Il y a également l' « Unité Child abuse » s'occupant de ce qui touche à la pédopornographie. Les Computer Crime Units (CCU) vont être intervenantes dans les dossiers. Ces unités vont remonter aux sources pour identifier les auteurs ou, après intervention de la police locale, vont intervenir dans l'analyse des supports découverts (ex : ordinateur, smartphone). Les supports vont passer par le laboratoire numérique et les données trouvées vont être fournies sous forme de rapport afin d'entendre les auteurs présumés sur base des éléments de preuve disponibles.
Une CCU Fédérale (FCCU) agit à partir du moment où les auteurs ne peuvent pas être territorialement localisés. Dans ce cas, elle est chargée de retrouver les auteurs. Mais, un magistrat peut désigner une CCU Régionale (RCCU). Il y en a une par arrondissement. En fonction du dossier et de sa localisation, c'est elle qui va le prendre en charge. Lorsque c'est l'environnement informatique qui est touché (hacking, piratage de données, etc.), les CCU sont les enquêteurs. Mais, lorsqu'il s'agit d'une récupération d'informations techniques dans le cadre d'une enquête classique, ils doivent les transmettre aux enquêteurs en charge qui continuent le travail.

Pouvez-vous m'éclairer sur les statistiques relatives au cyber-harcèlement de l'année 2019 ?

La Police Fédérale a publié, le 3 juillet 2019 le Moniteur de sécurité de 2018. Cela est très compliqué, car pour tout ce qui touche au numérique, énormément de personnes ne portent pas plainte. La criminalité informatique est en hausse, mais peu de victimes portent plainte. Il y a une grande différence entre les statistiques des dossiers ouverts et la réalité.

En pratique, dans le cas de cyber-harcèlement, est-ce que les méthodes particulières de recherche sont beaucoup utilisées ?

Pas forcément, car en général, l'identification des auteurs n'est pas trop complexe. Mais, s'il y a un VPN, le magistrat pourra les ordonner.

Annexe 3 : Interview du 15 juillet 2019 avec Philippe Van Linthout (Juge d'instruction du tribunal de première instance d'Anvers, division Malines et co-président de l'Association des juges d'instruction de Belgique)

Comment définiriez-vous le cyber-harcèlement ?

Le cyber-harcèlement rejoint le harcèlement sauf qu'il est encore plus fort, car automatisé. Les individus peuvent donc aller plus loin, plus fort, et être plus anonymes. L'ampleur est beaucoup plus grande. Le cyber-harcèlement est surtout incriminé sur base de l'article 145, paragraphe 3*bis*, de la loi du 13 juin 2005. Généralement cela commence par du harcèlement moral (dans la rue, dans les magasins, etc.) et cela devient par après, très souvent, du cyber-harcèlement. De nombreux cas d'application prennent place entre ex-partenaires. Soit cela reste dans le monde réel, soit cela passe dans le monde virtuel et, dès lors nous trouvons dans le cas de l'article 145, paragraphe 3*bis*, de la loi du 13 juin 2005.

Auparavant le harcèlement téléphonique était puni plus largement avec un emprisonnement pouvant aller jusque quatre ans. Mais, la Cour constitutionnelle a dit que cela n'était pas équitable et qu'il fallait punir le harcèlement téléphonique par un emprisonnement de deux ans maximum. Je ne comprends pas bien ce raisonnement, car on peut parler d'inégalité lorsqu'on traite des mêmes choses d'une différente manière, mais quand il y a des choses qui sont différentes, nous devons avoir la possibilité de les traiter différemment. Je ne suis pas convaincu par le fait de dire que déposer une rose devant la porte de quelqu'un pour lui prouver que nous sommes toujours là est la même chose que d'installer un robot sur Internet qui va envoyer à chaque seconde des e-mails ou téléphoner à une personne.

À quelle fréquence avez-vous des dossiers relatifs à cette problématique ?

Il y a peu de dossiers concernant le cyber-harcèlement. Les suspects, qui ont souvent des problèmes psychiques, deviennent de plus en plus spécialisés. Il devient de plus en plus difficile d'arrêter les faits et d'identifier le suspect. Les auteurs de ces faits de cyber-harcèlement ont désormais compris qu'il existe des accords pour demander l'identification lorsque l'envoi d'un e-mail est réalisé en utilisant Gmail, Hotmail, ou autres services

courants. Ils utilisent dès lors, à la place de ces services courants, des torts networks pour se rendre anonyme ou des e-mails jetables.

J'ai déjà envoyé des commissions rogatoires vers la Suisse par exemple, car l'intéressé utilisait un Protonmail. Il s'agissait d'une firme qui promettait à ses clients de pouvoir envoyer des e-mails sans qu'aucune trace ne soit gardée. Actuellement, après l'affaire Snowden, des firmes se profilent en disant que l'intimité des clients est sacrée et que par conséquent aucune preuve ne sera gardée. Heureusement, certaines firmes disent cela pour la publicité, mais restent conscientes que si elles aident des terroristes cela va porter atteinte à la société et gardent quand même des traces. Dans le cas d'espèce, la firme savait quand était le log in et log out du client, mais n'avait pas enregistré les adresses IP. Dans ces affaires-là, qui prennent beaucoup de temps et de capacité de recherche, je suis confronté à un suspect très doué et je suis certain que de plus en plus de personnes savent qu'en utilisant un tort il est très difficile de les identifier. Cela devient donc un grand problème.

Est-ce que cela concerne majoritairement des adolescents ou pas spécialement ?

Pas spécialement. Je suis uniquement juge d'instruction donc je ne vois que les adultes, mais par contre, je participe parfois à des entrainements ou à des discussions avec la police en ce qui concerne la jeunesse. Auparavant, les élèves se harcelaient dans la cour de récréation. Maintenant nous observons que les élèves, lorsqu'ils reçoivent leur smartphone, vont directement sur les réseaux sociaux tels qu'Instagram, Snapchat, etc. La première chose qui leur vient à l'esprit est qu'ils veulent être populaires. Ils veulent avoir le plus d'amis possible. Celui qui a le plus d'amis est le plus populaire. Ils sont insérés dans des groupes d'amis sur Internet. Cela devient une vie parallèle où la réputation est aussi importante que dans la vie réelle. Parfois ce sont les mêmes groupes d'amis, mais parfois il s'agit de groupes différents. Les likes ou les dislikes sont très importants et permettent au reste du groupe de savoir qui est la victime la plus facile à atteindre. Je pense que cela diffère chez les adultes, excepté peut-être pour les influenceurs.

Les écoles et les parents ont une grande responsabilité. J'ai participé à une réunion où l'on donnait des avis par rapport à l'usage d'Internet pour Child Focus. Il y avait des représentants des jeunes, mais aussi de Child Focus et Sensoa. L'idée est que si je rencontre une jeune fille, nous allons d'abord discuter, puis elle va faire des photos de son visage, puis en bikini et cela va de plus en plus loin jusqu'à ce qu'il y ait du sexe virtuel. Est-ce qu'il faut interdire cela ? Les représentants de Sensoa disent que non, que cela est devenu une partie de la vie, mais qu'il faut être conscient que si une personne souhaite

envoyer sa poitrine dénudée, il ne faut pas que son visage soit visible afin que cela ne puisse pas être utilisé contre elle par la suite.

Quelle est la procédure qui s'enclenche lorsqu'une personne dépose plainte pour cyber-harcèlement ?

Il y a une très grande différence entre les zones de police. Il fut un temps où lorsqu'une personne se présentait à la police en expliquant qu'elle avait subi un problème via Internet et qu'elle avait gardé la preuve et disposait de l'adresse IP, la personne derrière le guichet ne comprenait pas la signification d'une adresse IP. Cela signifie que dès le moment où on notait la plainte, c'était déjà perdu, car nous ne savions pas ce qui devait être demandé, sauvegardé, etc. Lorsque quelqu'un dépose plainte à la police, celle-ci doit avertir la victime de plusieurs choses notamment du fait qu'il faut disposer de la preuve de la menace, mais également des traces techniques. J'espère, mais je ne suis pas convaincu que cela est déjà le cas dans toutes les zones de police. Si je vous envoie un e-mail et que vous souhaitez utiliser cet e-mail comme élément de preuve, la seule impression de celui-ci ne suffit pas. Cela peut être un début de preuve, mais cela a pu être copié dans Word et être modifié. Comment prouver que cela vient de telle personne ? En cinq minutes de temps, je peux m'envoyer des e-mails en faisant croire qu'ils proviennent d'une autre personne. Nous avons besoin des informations techniques étant derrière le mail. Ou bien elles sont imprimées avec l'e-mail, ou bien les victimes doivent savoir que c'est mieux de sauvegarder le document digital comme élément de preuve. Si je forward un e-mail qui me menace, les informations techniques vont disparaître. Par contre, si je l'ajoute en pièce jointe, les informations vont être intégrées à l'e-mail. Il est très important que les policiers sachent comment agir face à une victime « d'Internet ».

Par exemple, la situation suivante est très urgente : une jeune fille se présente à la police, car elle avait envoyé à son copain des photos de sa poitrine. Son copain lui avait demandé d'envoyer des photos de son vagin et lui avait dit que si elle refusait, il diffuserait les photos de sa poitrine. Si on ne réagit pas tout de suite et que les photos sont envoyées, cela peut avoir de graves conséquences. La police peut aller chez le jeune homme afin d'effacer les photos. Mais si lui les envoie à plusieurs amis qui les publient sur divers sites, il est trop tard. C'est une question d'urgence. Il est très important de savoir comment réagir. La procédure sera de bien pouvoir évaluer de quoi on parle. Si cela est quelque chose de très urgent comme la menace d'une diffusion sur internet, il faut agir, s'adresser au procureur ou au juge d'instruction afin de faire une perquisition, car les dégâts peuvent être immenses.

J'aborderai le sujet dans une émission qui sera diffusée prochainement. Lors de cette émission, une femme d'une vingtaine d'années était en larmes, car elle n'osait pas dire à sa famille qu'une vidéo avait été enregistrée avec son consentement, dans une relation et que le garçon a diffusé la vidéo à son insu. Il s'agit d'un cas de *revenge porn*. La jeune femme avait engagé un expert en informatique pour voir s'il existait des traces afin de savoir qui était le premier à avoir lancé la vidéo. L'expert a montré que la même vidéo était des milliers de fois copiée et les titres de la vidéo différaient en fonction des sites. Une vidéo est un fichier digital qui se trouve sur un serveur quelque part dans le monde. Il est très important de voir ce qu'il y a comme éléments de preuve, et dans certains cas, devoir dire aux gens que cela n'est pas possible. Parfois, des personnes viennent me voir en disant qu'ils ont la preuve, qu'ils ont une adresse IP. Mais cela ne veut rien dire, car une adresse IP c'est comme un jeton pour aller dans une attraction à la foire. Vous avez votre tour et une fois que vous sortez le jeton est donné à quelqu'un d'autre. Il faut avoir une date, une heure et un fuseau horaire pour voir dans quel pays on est. Une heure fait la différence entre telle et telle personne. Il est primordial d'avoir des personnes entraînées afin d'informer les gens, sauvegarder les éléments de preuve et pouvoir sonner l'alarme si c'est nécessaire.

Concernant l'élément matériel du harcèlement moral, faut-il selon vous une répétition des actes litigieux ? Selon un arrêt de la Cour de cassation de 2013, un acte unique de nature incessante et répétitive suffit. Êtes-vous d'accord avec cette interprétation extensive ?

Absolument. Pour moi le harcèlement moral protège le droit d'une personne de se trouver chez elle sans être ennuyée. À mon avis, même un acte pourrait suffire. Par exemple, une rose déposée devant une porte avec toute une histoire derrière. Le but étant de montrer « j'étais à la porte, je suis à côté de toi ». Pour moi l'idée derrière est de se demander si la personne était au courant qu'elle allait ennuyer l'autre personne et perturber son calme.

Il existe une controverse quant à la nécessité d'y avoir une répétition de comportements en ce qui concerne le harcèlement téléphonique. Quel est votre avis ?

En pratique, si c'est à l'aide d'un moyen électronique, on voit presque toujours une répétition d'actes.

Plusieurs dispositions (ex : 46bis et 88bis C.i.cr.) énoncent l'obligation de collaboration des opérateurs et des fournisseurs de communications électroniques. Les réseaux sociaux tels que *Facebook* et *Instagram* sont-ils visés par ces dispositions ?

Oui. C'était déjà clair auparavant, mais il y a trois moments dans l'histoire qui ont apporté beaucoup de changement. Premièrement il y a l'arrêt Yahoo de la Cour de Cassation qui concerne l'article 46*bis* du Code d'instruction criminelle. Dans cet arrêt la cour a dit à Yahoo qu'il était virtuellement présent en Belgique, qu'il y gagne financièrement, comme d'autres opérateurs ayant leur siège en Belgique. La cour a dit que le siège n'est pas le plus important, ce qui compte c'est d'être présent virtuellement. L'idée derrière est qu'on ne peut pas seulement profiter de notre territoire, il y a également des obligations à respecter. À partir du moment où un opérateur est actif sur le territoire belge, il faut respecter les obligations qui s'en suivent. À la suite de cet arrêt, j'ai lancé une écoute téléphonique à l'égard de deux belges qui utilisaient l'application *Skype* pour communiquer. La Cour de cassation a confirmé que *Skype* était dans l'obligation de collaborer. Avec la loi du 25 décembre 2016, la loi a été modifiée et une définition extrêmement large y a été insérée. C'est la jurisprudence Yahoo qui a été mise dans la loi. Est-ce que cela est déjà applicable en pratique ? C'est une autre question.

Quelle est la différence entre l'article 39ter du Code d'instruction criminelle et l'article 126 de la loi du 13 juin 2005 ? Tous deux parlent de conservation/préservation de données. Quelles sont les personnes physiques et morales visées par l'article 39ter ?

L'article 126 de la loi de 2005 concerne la conservation de données pour le territoire belge. Cela concerne tous les opérateurs et tous ceux qui sont actifs sur le territoire belge. De manière large cette disposition s'applique aux firmes actives en Belgique qui doivent donc conserver leurs données. Ce n'est pas une loi pénale, c'est une loi sur l'organisation des télécommunications.

À côté de ça, nous avons les articles qui énoncent le fonctionnement des recherches dans les systèmes informatiques. Il y a l'identification régie par l'article 46*bis* du Code d'instruction criminelle et le repérage régi par l'article 88*bis* du même Code. Le Code d'instruction criminelle est un code autonome qui nous donne l'autorisation de demander les données. Si les données sont présentes, nous pouvons les saisir, mais pour être certain qu'elles soient présentes, il y a la loi sur les télécommunications.

Entre temps, le législateur belge a constaté que nous avions ratifié la Convention sur la cybercriminalité, mais que nous n'avions pas encore inséré dans notre Code d'instruction criminelle deux articles que tous les pays ayant ratifié la Convention doivent mettre dans leur Code. Dans le monde digital, tout part très vite. Dans cette convention, il est prévu que les données doivent être conservées rapidement et que par après, il peut être demandé de les saisir. L'article 39*ter* concerne les données demandées à la Belgique et le 39*quater* celles demandées à un autre pays. Il existe d'autres moyens de saisir des informations,

mais, lorsqu'il est nécessaire d'avoir les informations très rapidement, il est préférable d'avoir une législation qui les règle. La loi est entrée en vigueur en janvier 2017. Avant janvier 2017, est-ce qu'on perdait tout ? Non on téléphonait aux fournisseurs en leur demandant de mettre les données de côté, mais, dû à la Convention, c'est maintenant bien réglé.

Je ne pense pas utiliser l'article 39*ter* vis-à-vis de Proximus, car c'est tellement clair que Proximus est la firme devant collaborer avec moi sur base de l'article 46*bis* et 88*bis*. Est-ce que l'article 39*ter* est souvent utilisé ? Je ne crois pas. C'est seulement pour ceux qui diraient qu'ils ne collaborent pas avec des externes. Dès lors nous avons une base légale pour leur demander les informations utilisables pour l'enquête digitale. L'article 126 de la loi du 13 juin 2005 est à part, il énonce la durée de sauvegarde.

La Cour d'appel d'Anvers, chambre des mises en accusation a rendu un arrêt en décembre 2017 au sujet de l'article 88quater du Code d'instruction criminelle. Selon elle, le paragraphe 1er de cet article peut s'appliquer à l'inculpé en l'obligeant de dévoiler le code pin de son téléphone portable. Que pensez-vous de cette interprétation ? Cela s'appliquerait donc également au code de verrouillage du téléphone ?

Oui cela s'applique également au code de verrouillage du smartphone. La jurisprudence pour l'instant va dans tous les sens. J'avais un client qui était en prison, car nous avions découvert des kilos de cocaïne. Nous avions également trouvé un BlackBerry équipé avec verrouillage. J'ai dit que cela serait vraiment utile pour analyser le network. J'ai demandé au client de donner son mot de passe. Il a refusé. Le parquet l'a emmené devant moi pour ce délit consistant à refuser de divulguer son mot de passe. Je me suis alors demandé s'il y avait un danger de récidive. J'ai donc redemandé au monsieur de donner son mot de passe. Il a à nouveau refusé. Il a donc commis le délit pour une seconde fois. Je lui ai demandé pour la troisième fois s'il était sûr. Il a refusé à nouveau. Je l'ai donc mis sous mandat d'arrêt.

Cette affaire a été devant la chambre du conseil où l'avocat a dit que ce n'était pas démocratique, qu'il s'agissait d'une violation des droits de l'homme. Ils sont allés en appel. La Cour d'appel d'Anvers, chambre des mises en accusation, a libéré l'homme et a dit qu'il était impossible d'obliger un inculpé à divulguer son code. Le parquet est lui-même allé en appel et la même chambre des mises en accusation, autre composition, a dit que l'inculpé était obligé de divulguer son mot de passe.

Il y a deux arrêts récents, un arrêt disant que c'est possible, un autre disant que ça ne l'est pas. La Cour d'appel d'Anvers a posé une question préjudicielle à la Cour

constitutionnelle en demandant s'il n'existait pas une discrimination entre le paragraphe un et deux de l'article 88*quater*. Selon moi, cela n'a rien à voir avec le droit de ne pas s'auto-incriminer. Le droit de ne pas s'auto-incriminer vise les déclarations faites par l'inculpé. Cela s'explique historiquement par le fait qu'on ne voulait pas des déclarations obtenues par la torture ou de fausses déclarations dues à la peur. Dans le cas d'espèce, il ne s'agit pas de déclarations. Nous ne demandons pas à l'inculpé de dire quelque chose. Nous demandons le mot de passe et pas de nous montrer où se trouvent les fichiers, nous allons les chercher nous-mêmes dans l'ordinateur ou le smartphone. Il est même possible qu'il existe des choses à décharge dans l'ordinateur que l'inculpé avait oublié de mentionner.

Dans l'arrêt historique Saunders, il est clair qu'il n'est pas possible de refuser toutes les choses demandées par la justice. Si je me fais arrêter par la police pour un contrôle d'alcoolémie. L'agent me demande si j'ai bu et de souffler, je ne peux pas refuser de le faire sous prétexte que je m'auto-incrimine. Cela est punissable en Belgique. Un autre exemple est celui de l'ADN. L'ADN est une trace qui pourrait me lier à cent meurtres ayant été commis. Je peux refuser de fournir mon ADN, mais le juge d'instruction peut décider de le prélever quand même. Encore un autre exemple est celui des empreintes digitales. La différence entre les paragraphes un et deux est très explicable. Le premier paragraphe concerne le fait de demander le mot de passe d'un ordinateur et rien d'autre. Le deuxième paragraphe vise, quant à lui, le fait de demander de montrer des éléments dans l'ordinateur. Il y a des conclusions divergentes dans la jurisprudence.

Quelles sont les méthodes les plus utilisées afin de récolter les preuves électroniques en matière de cyber-harcèlement ?

La cyber-infiltration n'est pas encore utilisée en pratique. Nous sommes occupés à former les policiers. La cyber-infiltration est un outil qui doit être rapidement et grandement utilisé. Par exemple, dans une affaire de pédopornographie, au moment où je vois que l'auteur est en train de discuter sur le net avec un autre enfant, il faudrait une réaction instantanée. Une police locale devra d'abord reconnaitre la situation « le chat est ouvert, c'est une chance unique de voir le réseau ». À partir du moment où je ferme l'ordinateur, c'est trop tard. Même si on obtient le mot de passe par après, on ne sera jamais dans le même *chat group*. Chaque recherche de chaque ville devrait avoir quelqu'un en stand-by à qui l'on ferait appel au moment adéquat.

Les articles que nous utilisons le plus souvent sont les articles 39*bis* et 88*ter*. La renaissance de l'article 88*ter* s'explique par la loi du 5 mai 2019. L'article 39*bis* a été modifié par la loi du 25 décembre 2016. Par après, cette loi a été partiellement annulée

par l'arrêt du 6 décembre 2018. Cet arrêt a annulé le paragraphe trois de l'article 39*bis*. Cela devait avoir pour conséquence de faire renaitre l'article 88*ter* qui avait disparu. Mais comme la situation n'était pas claire, la loi du 5 mai 2019 a réinstallé et modifié légèrement l'article 88*ter*. Il faut dorénavant assembler l'article 39*bis* et 88*ter*. Ce qui est clair désormais c'est que les recherches sur les réseaux relèvent de la compétence du juge d'instruction et plus de celle du parquet.

Est-ce que la police peut ouvrir l'application WhatsApp ? Y a-t-il une grande différence dans les faits entre l'application WhatsApp et des SMS ? Quelle est la différence dans l'ingérence de la vie privée entre les deux? Ma seule critique à l'égard de cet arrêt est qu'il n'est pas logique. Lorsqu'on regarde dans les photos ainsi que les SMS se trouvant sur un smartphone, il y a des chances d'en découvrir beaucoup plus que lors d'une perquisition. Mais la Cour constitutionnelle dit que lorsqu'on fait le lien vers le serveur, cela touche tellement à l'intimité que cela doit être comparé à la perquisition domiciliaire et à l'écoute. Mais lorsque je mets le portable en mode avion, n'y a-t-il malgré tout vraiment rien à cacher ? Les messages sont là et certaines applications pourront s'ouvrir malgré le mode avion. La cour devrait donc considérer que pour toute analyse de smartphone il faut un juge d'instruction. Mais cela serait impossible.

Lorsqu'il y a la commission d'un harcèlement moral cumulé à du harcèlement téléphonique, est-ce que vous privilégieriez plutôt l'article 442*bis* ou l'article 145, paragraphe 3*bis*, de la loi du 13 juin 2005 ?

Il faut toujours mettre l'étiquette adaptée pour l'infraction. L'article 145, paragraphe 3*bis*, de la loi du 13 juin 2005 est un article passe-partout. Le harcèlement moral est large, il peut être aussi électronique. Cela dépend également de l'arrondissement. Certains disent que si cela est clair qu'il s'agit du harcèlement moral, basons nous sur l'article 442*bis* sans discuter des « problèmes » que peut engendrer l'article 145, paragraphe 3*bis*, de la loi du 13 juin 2005. D'autres arrondissements distinguent très clairement les deux dispositions. Il y a un grand problème avec les délits de presse. Il y a une discussion hallucinante. Les délits de presse existent depuis 1800 dans des atmosphères politiques exaltantes. Les personnes utilisaient des machines à papier afin de se révolter contre le Roi ou le Président. Nous sommes en train d'évoluer. Mais je ne comprends pas comment on peut dire qu'exprimer des propos au moyen d'Internet est la même chose qu'utiliser des grandes machines afin d'imprimer des tracts. Sauf pour le racisme et la xénophobie, il y a un délit de presse lorsque l'expression d'une opinion (par exemple des menaces, de la calomnie ou de la diffamation) est réalisée par un moyen associé aux grandes machines de l'époque. Par contre, à mon avis, l'article 145, paragraphe 3*bis*, de la loi du 13 juin 2005 ne parle pas d'une expression. Dès lors, l'expression d'un sentiment via Internet est un délit de presse. Par contre, si je le fais électroniquement et qu'à cause de cela la victime peut

prouver qu'elle a subi des dommages, dès lors cela n'a rien à voir, selon moi, avec une opinion exprimée, mais avec le fait qu'un réseau a été utilisé afin d'endommager quelqu'un. Et cela ne sera par conséquent pas un délit de presse. Il y a eu un jugement à Bruxelles qui a été devant la Cour d'appel où il a été dit que cela correspondait également à un délit de presse, mais, selon moi, cela n'est pas logique. J'attends l'interprétation de la Cour de Cassation sur ce point-là.

D'après vous, la législation actuelle est-elle adaptée ou serait-il judicieux de la modifier ?

Pour l'instant, la législation est adaptée. Je ne pense pas que cela soit facile de réglementer le cyber-harcèlement. J'attends toujours les interprétations de la Cour constitutionnelle, également au sujet de la conservation de données qui est très importante. Dans tous les crimes et délits que vous avez mentionnés, j'ai besoin de la preuve, car si celle-ci est « jetée » après quelques mois, je n'ai plus la possibilité de la retrouver. Maintenant, il faut avouer que cela ne veut pas dire que dans la pratique ça fonctionne. La loi m'autorise techniquement beaucoup de choses en tant que juge d'instruction, parfois avec l'aide de la police, mais dans certains cas, c'est tellement compliqué, les données sont tellement cryptées qu'il m'est quasiment impossible d'y accéder. Par exemple, sur les écoutes téléphoniques on n'entend presque plus rien.

Selon vous, serait-il pertinent d'adopter une loi particulière en la matière ?

Non. Pour ceux qui connaissent le Code d'instruction criminelle, il est facile de retrouver les dispositions. Par contre, cela est problématique si on continue à ajouter très rapidement des infractions dans le Code au point où les citoyens ne savent pas qu'elles existent. Je ne suis pas pour l'idée de lancer un tout nouveau Code pénal ou Code d'instruction criminelle. Si ce jour arrive, c'est à ce moment-là qu'il y aura de vrais problèmes, car chaque juriste aura une opinion sur chaque nouvel article.

Quelles solutions devraient être développées, dans le futur, afin de lutter contre ce phénomène ?

Tout d'abord il faut que les cours clarifient certaines dispositions. Ensuite, il faut éviter, au moyen de l'éducation, que cela se produise. Il faut sensibiliser les gens aux conséquences que cela peut avoir et aux difficultés d'arrêter la propagation de contenus dans certains cas. Il faut pouvoir expliquer aux personnes pourquoi certaines choses sont nécessaires comme la conservation des données.

Que pensez-vous d'une inscription sur les réseaux sociaux sur base du registre national ? Cela serait-il un moyen adéquat afin de contrer l'anonymat ?

Cela serait un rêve. Par contre concernant l'anonymat, il faut faire une distinction. Il y a beaucoup de situations où l'anonymat est une bonne chose. Par contre, si en me servant de cet anonymat, je décide de commettre des infractions, au moyen d'une adresse IP ne portant pas mon nom, là, l'identification doit être possible. Toutes les connexions vers Internet ne peuvent pas être anonymes. Il faut qu' on puisse identifier l'auteur si une infraction a lieu. L'anonymat ne peut pas être absolu, car il y a plein de faits se déroulant sur Internet, ou au moyen d'Internet (par exemple via *Viber* ou *Télégram*) pour, entre autres, organiser des infractions dans le « monde réel ».

LOUVAIN-LA-NEUVE | BRUXELLES | MONS | TOURNAI | CHARLEROI | NAMUR
Place Montesquieu, 2 bte L2.07.01, 1348 Louvain-la-Neuve, Belgique | **www.uclouvain.be/drt**