MONDIALISATION ET INTERNET
Belgique

Prof. dr. Eva Lievens
Université de Gand

I / Mondialisation, Internet et les droits des individus

A) Protection des données personnelles

La loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (LVP) contient la transposition de la Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 concernant la protection des personnes physiques quant au traitement de données à caractère personnel et à la libre circulation de ces données (Directive sur la protection des données personnelles).[1] Par « données à caractère personnel », il convient d'entendre toute information concernant une personne physique identifiée ou identifiable. Est réputée « identifiable » une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale (art. 1, §1). Quelques exemples de données à caractère personnel sont : un nom, une photo, un numéro de téléphone, une adresse e-mail ou une empreinte digitale.

La loi prescrit que, dans le cadre des données à caractère personnel la concernant, toute personne physique a droit à la protection de ses libertés et droits fondamentaux, notamment à la protection de sa vie privée (art. 2). Le traitement de données à caractère personnel automatisé (art. 3, §1),[2] donc à l'aide de technologies de l'information (informatique, réseaux de télécommunication, Internet), est dès lors soumis à certaines conditions.

La loi prescrit que le traitement des données à caractère personnel n'est autorisé que dans certains cas : a) lorsque la personne concernée a indubitablement donné son consentement,[3] b) lorsqu'il est nécessaire à l'exécution d'un contrat, c) lorsqu'il est nécessaire au respect d'une obligation légale, c) lorsqu'il est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée, d) lorsqu'il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, e) lorsqu'il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le tiers auquel les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée (art. 2).

La loi ne s'applique pas au traitement de données à caractère personnel effectué pour l'exercice d'activités exclusivement personnelles ou domestiques (art. 3, §2). Certains articles de la loi ne s'appliquent pas aux traitements de données à caractère personnel effectués aux

[1] Cette réglementation sera fondamentalement réformée par le Règlement général sur la protection des données. Pour de plus amples informations, cf. http://data.consilium.europa.eu/doc/document/ST-5419-2016-REV-1/fr/pdf.
[2] La loi peut également s'appliquer au traitement non automatisé de données à caractère personnel (art. 3, §1).
[3] Art. 1, §8 prescrit que par « consentement de la personne concernée », on entend « toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée ou son représentant légal accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement ».

seules fins de journalisme ou d'expression artistique ou littéraire, ou par des services de sécurité, de police et autres services publics (art. 3, §3-7).

En principe, le traitement de données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la vie sexuelle, de données à caractère personnel relatives à la santé et les données de nature judiciaires est interdit (art. 6, §1, art. 7, §1 et art. 8, §1). Ces règles font l'objet d'une série d'exceptions visées à l'art. 6, §2 et 3, à l'art. 7, §2 et à l'art. 8, §2.

Pour ce qui est de la transmission des données personnelles à l'étranger, trois situations sont possibles. Les données à caractère personnel peuvent être transférées vers un État membre de l'Union européenne si la LVP le justifie et vers des pays non membres de l'UE si le pays en question assure un niveau de protection adéquat et moyennant le respect de la LVP (art. 21, §1). Le caractère adéquat du niveau de protection est déterminé par la Commission européenne. Le transfert de données à caractère personnel vers un pays non membre de la Communauté européenne n'assurant pas un niveau de protection adéquat, peut être effectué dans les cas visés à l'art. 22. Ainsi, la personne concernée peut indubitablement donner son consentement au transfert envisagé ou des contrats peuvent être conclus par le responsable du traitement, qui doivent être approuvés par Arrêté royal, après avis de la Commission de la protection de la vie privée, sauf si les contrats types établis par la Commission européenne sont utilisés.

Le contrôle du respect des dispositions légales est exercé par la Commission de la protection de la vie privée (ou : Commission vie privée)[4] (art. 23). Elle peut émettre des avis (art. 29), formuler des recommandations (art. 30), examiner des plaintes (art. 31) et elle octroie des autorisations (art. 36bis). La Commission vie privée peut aussi accomplir des missions de médiation. Si nécessaire, la Commission peut dénoncer au procureur du Roi les infractions dont elle a connaissance ou soumettre tout litige au tribunaux civils. Les infractions aux dispositions de la LVP peuvent donner lieu à des sanctions pénales (Chapitre VIII).

Outre la LVP, la loi du 13 juin 2005 relative aux communications électroniques (LCE) contient également des dispositions pertinentes pour le traitement des données à caractère personnel. L'article 129 LCE fixe par exemple les conditions d'utilisation des cookies.[5]

En mai 2015, la Commission vie privée a formulé une **Recommandation d'initiative concernant 1) Facebook, 2) les utilisateurs d'Internet et/ou de Facebook ainsi que 3) les utilisateurs et fournisseurs de services Facebook, en particulier les 'plug-ins' sociaux** (Recommandation n° 04/2015, du 13 mai 2015).[6] Cette recommandation a été émise suite à l'entrée en vigueur des nouvelles conditions d'utilisation imposées par Facebook à partir du 30 janvier 2015. Dans sa recommandation, la Commission vie privée se déclare compétente

[4] https://www.privacycommission.be.
[5] Voir également la Recommandation d'initiative concernant l'utilisation des cookies (Recommandation n° 01/2015, 4 février 2015) de la Commission vie privée : https://www.privacycommission.be/sites/privacycommission/files/documents/recommandation_01_2015_0.pdf.
[6] https://www.privacycommission.be/sites/privacycommission/files/documents/recommandation_04_2015.pdf. Cette recommandation est étayée par une étude menée par la KU Leuven (CiTiP and COSIC) et VUB (SMIT) : From social media service to advertising network A critical analysis of Facebook's Revised Policies and Terms, 2015, https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-2.pdf.

pour ce qui est du traitement par Facebook des données à caractère personnel des utilisateurs belges (point 56). La recommandation met l'accent sur l'utilisation et la collecte de données par Facebook au moyen de cookies et de plug-ins sociaux. La Commission affirme que Facebook doit faire toute la transparence sur l'utilisation des cookies et elle encourage Facebook à renoncer au placement systématique de cookies d'identification unique de longue durée chez les non-utilisateurs (en ce compris les utilisateurs déconnectés ou désactivés) de Facebook, sauf si elle obtient à cet effet le consentement indubitable et spécifique des personnes concernées via un opt-in et dans la mesure où cela est strictement nécessaire pour des finalités légitimes. La même autorisation par opt-in (et pas par opt-out) doit être obtenue pour les utilisateurs de Facebook.

Dans la mesure où Facebook ne souhaitait pas suivre les recommandations susmentionnées, le 10 juin 2015, la Commission vie privée a lancé une procédure en référé. Dans son jugement du 9 novembre 2015, le président du Tribunal de première instance de Bruxelles a fait droit à la Commission vie privée. Le tribunal a confirmé l'applicabilité du droit belge et la compétence des juridictions belges. Le président a constaté une violation manifeste de la législation belge sur la protection des données et il a ordonné à Facebook de cesser 1) de placer des cookies (plus particulièrement un « datr-cookie ») sur le système des non-utilisateurs de Facebook en Belgique lorsqu'ils aboutissent sur un site web du domaine Facebook, sans les informer suffisamment et adéquatement au préalable du fait que Facebook enregistre le cookie, ainsi que de l'usage que Facebook fait de ces cookies par le biais des plug-ins sociaux et 2) à la collecte des cookies par le biais de plug-ins sociaux placés sur des sites web de tiers. Facebook a interjeté appel de ce jugement. Depuis lors, la Commission vie privée a intenté une procédure sur le fond contre Facebook au début de l'année 2016.

L'arrêt *Google Spain* de la Cour de justice de l'Union européenne[7] a fait couler beaucoup d'encre. Il touche essentiellement à ce que l'on appelle le « droit à l'oubli », qui est cité dans ce contexte, soit un droit à la suppression de certaines données à caractère personnel lorsque leur traitement n'est pas conforme aux dispositions de la Directive sur la protection des données personnelles.[8] Ce droit à la suppression est également prévu par l'art. 12 de la LVP belge, en cas « des raisons sérieuses et légitimes tenant à une situation particulière ». Une personne peut adresser une demande au gestionnaire d'un site web afin d'obtenir la suppression de certaines données à caractère personnel suivant une procédure déterminée. Si le gestionnaire ne souhaite pas accéder à la demande, la personne peut également s'adresser à Google ou à un autre moteur de recherche qui propose des services aux citoyens belges. Google prévoit à cette fin un formulaire en ligne disponible dans plusieurs langues.

B) La liberté d'expression sur Internet

Les articles 19, 25 et 150 de la Constitution belge contiennent diverses garanties constitutionnelles relatives à la liberté d'expression et à la liberté de la presse. Ainsi, l'art. 19 prescrit que « la liberté de manifester ses opinions en toute matière » est garantie « sauf la répression des délits commis à l'occasion de l'usage de ces libertés », et l'art. 25 garantit que « la presse est libre ; la censure ne pourra jamais être établie [...] ». Dans un arrêt du 6 mars

[7] C-131/12, 13 mai 2014.
[8] Jef Ausloos en Brendan Van Alsenoy, Note sous HJEU (Grande chambre) 13 mai 2014, *Auteurs & Media* 2014, 5, 411-416.

2012, la Cour de cassation a affirmé que les textes publiés sur Internet peuvent être jugés comme des délits de presse,[9] puisque la diffusion numérique peut être considérée comme un procédé similaire à celui d'une presse. Les discours oraux qui sont diffusés par des médias audio-visuels ou en ligne (par exemple dans des vidéo YouTube) ne peuvent être sanctionnés au titre de délit de presse.[10] Aux termes de l'art. 150 C., les délits de presse doivent être jugés par la Cour d'Assises, à l'exception des délits de presse inspirés par le racisme ou la xénophobie. Depuis la Deuxième guerre mondiale, seulement deux affaires ont effectivement été soumises à cette juridiction, de sorte que l'on peut affirmer que les délits de presse, même par Internet, jouissent d'une immunité pénale *de facto*.[11] Cela n'enlève rien au fait que certaines opinions punissables exprimées sur Internet peuvent être poursuivies s'il n'est pas satisfait aux quatre conditions pour pouvoir être considéré comme délit de presse (à savoir 1) un avis ou une opinion qui 2) est punissable par la loi et 3) est rendue publique par 4) un média imprimé), par exemple s'il s'agit simplement d'une information ou d'une illustration et pas d'un avis ou d'une opinion. De plus le régime de la responsabilité civile en vertu de l'article 1382 du Code civil (C.civ.) peut également être invoqué pour s'opposer à des publications illicites sur Internet et, par exemple, obtenir une indemnité.

C) Autres droits

Le droit au respect de la vie privée est explicitement garanti par l'art. 22 de la Constitution belge. Ce droit s'applique également à l'Internet. Les journalistes ne peuvent pas davantage violer le droit au respect de la vie privée dans les publications sur Internet, quand bien même les personnages publics doivent se montrer plus tolérants que les particuliers.[12] Le droit à l'image s'applique également à l'Internet. Toute violation de ce droit peut donner lieu à une indemnisation. Certaines violations du droit au respect de la vie privée sont par ailleurs punissables, même lorsqu'elles sont commises sur Internet. Ainsi, l'art. 378bis du Code pénal (C.pén.) prescrit que « *[l]a publication et la diffusion par le livre, la presse, la cinématographie, la radiophonie, la télévision ou par quelque autre manière*[13]*, de textes, de dessins, de photographies, d'images quelconques ou de messages sonores de nature à révéler l'identité de la victime du [voyeurisme, de l'attentat à la pudeur et du viol] sont interdites, sauf si cette dernière a donné son accord écrit ou si le procureur du Roi ou le magistrat chargé de l'instruction a donné son accord pour les besoins de l'information ou de l'instruction* ». Fin janvier 2016, un nouvel article 371/1 a été ajouté au Code pénal. Cet article vise à sanctionner le voyeurisme et à lutter contre le phénomène de « *porno vengeance* ». Ce phénomène concerne le partage et la diffusion de matériel sexuellement explicite (souvent d'ex-partenaires) sans autorisation. Il se manifeste principalement dans l'environnement en ligne : sur les plates-formes de média sociaux (par exemple Facebook ou YouTube), sur des sites pornographiques classiques ou sur des sites Internet spécialisés de « porno vengeance » ou encore par des applications photo et vidéo sur les smartphones. L'art. 371/1 punit le fait de montrer, rendre accessible ou diffuser « *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* ».

La loi du 11 mars 2003 sur certains aspects juridiques des services de la société de

[9] Cass. 6 mars 2012, *Auteurs & Media* 2012, 2/3, 253.
[10] Cass. 29 octobre 2013, *T.Strafr.* 2014, 2, 142.
[11] Dirk Voorhoof et Peggy Valcke, Handboek Mediarecht, Larcier, 2014, 104-106.
[12] Dirk Voorhoof et Peggy Valcke, Handboek Mediarecht, Larcier, 2014, 236-238.
[13] Donc également sur Internet.

l'information (également appelée : loi sur le commerce électronique)[14] a été intégrée fin 2013 au Livre XII « - Droit de l'économie électronique » dans le Code de droit économique (CDE). Le chapitre 6 de ce livre porte sur la responsabilité des prestataires intermédiaires. Une exemption de responsabilité est prévue dans le cas de « mere conduit » (activité de simple transport) (art. XII.17), *caching* (activité de stockage sous forme de copie temporaire de données) (art. XII.18) et *hosting* (art. XII.19). Dans le cas du hosting, cette exemption est uniquement valable 1° si le prestataire n'a pas une connaissance effective de l'activité ou de l'information illicite, ou, en ce qui concerne une action civile en réparation, s'il n'a pas connaissance de faits ou de circonstances laissant apparaître le caractère illicite de l'activité ou de l'information (en ce qui concerne une action en dommage) ou 2° si le prestataire agit promptement, dès le moment où il a de telles connaissances, pour retirer les informations ou rendre l'accès à celles-ci impossible et pour autant qu'il les communique sur le champ au procureur du Roi. L'art. XII.20 prescrit que les prestataires n'ont aucune obligation générale de surveiller les informations qu'ils transmettent ou stockent, ni aucune obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites.

D) Cyber-délits

Le Code pénal belge rend punissable une série de délits informatiques spécifiques : à savoir le faux en informatique (art. 210bis ; par exemple : la création d'un compte de courriel au nom d'une autre personne et l'envoi d'un courriel à partir de cette adresse e-mail à un tiers : Corr. Dendermonde, le 28 novembre 2005), fraude informatique (art. 504quater ; par exemple l'abus de la carte bancaire d'autrui : Corr. Arlon, le 9 mai 2005), accès non-autorisé à des systèmes informatiques (art. 550bis; hacking) et sabotage de données (art. 550ter). Il existe en outre une série de délits « classiques » susceptibles d'être également commis par la technologie numérique ou l'Internet, par exemple la production, la diffusion, la possession ou la consultation de pornographie infantile (art. 383bis C.pén. ; infra), atteintes portées à l'honneur ou à la considération des personnes (art. 443 et 444 C.pén.), le racisme, la discrimination et le sexisme (loi contre le racisme, loi anti-discrimination, loi genre et loi contre le sexisme), escroquerie (art. 496 C.pén.), et le délit de contrefaçon (art. XI.293 CDE). En principe, le tribunal correctionnel est compétent pour juger de ces délits, à l'exception de ceux qui sont considérés comme des délits de presse (supra). Aux termes de l'art. 139 du Code de procédure pénale (C.instr.crim.), est également compétent, le tribunal du lieu de l'infraction, celui de la résidence de l'inculpé, celui du siège social de la personne morale, celui du siège d'exploitation de la personne morale et celui du lieu où l'inculpé a été trouvé. Pour déterminer le lieu où le délit a été commis, la théorie objective de l'ubiquité et la doctrine de l'indivisibilité sont appliquées.[15] Les victimes peuvent se constituer partie civile dans la procédure pénale (art. 4 Titre préliminaire C.instr.crim.), ou elles peuvent s'adresser au tribunal civil pour une demande en indemnisation pour le préjudice subi si elles ne sont pas intervenues dans la procédure pénale ou si le parquet a classé l'affaire.

II / Mondialisation, Internet et la puissance des acteurs

[14] Cette loi a mis en œuvre la Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« Directive sur le commerce électronique »).
[15] Philippe Van Linthout, « Territoriale bevoegdheid in cyberspace », *T.Strafr.* 2009, 2, 113-114.

Le 16 décembre 2015, la Commission des clauses abusives a publié un **avis sur les conditions générales des sites de réseaux sociaux** (CCA 38)[16]. Cette commission a pour tâche de donner des avis et recommandations concernant les clauses et conditions contenues dans les contrats conclus entre les vendeurs et les consommateurs. Elle veille à prévenir toute clause irrégulière, à savoir des clauses qui semblent perturber manifestement l'équilibre entre les droits et les obligations des parties, elle peut recommander une formulation compréhensible des conditions contractuelles, ainsi que l'introduction de mentions ou de clauses qui lui semblent nécessaires pour obtenir une rédaction compréhensible.[17]

L'avis relatif aux conditions générales des sites de réseaux sociaux a été demandé par les organisations de consommateurs. Il débute par une analyse visant à savoir si le droit des consommateurs en matière de clauses irrégulières (art. VI.82 CDE e.s.) est applicable à la relation entre les sites de réseaux sociaux (comme Facebook, Google+, Twitter et Instagram) et les consommateurs belges. La Commission conclut que dans les cas où les sites de réseaux sociaux déclarent d'application d'un autre droit que le droit belge (comme le droit de l'État américain de Californie, États-Unis), les consommateurs belges peuvent avoir recours au droit d'un autre pays si le droit d'un autre État offre au consommateur une plus grande protection que le droit belge (art. VI.84 §2 CDE et l'article 6 du Règlement Rome I). Toutefois, étant donné que les sites de réseaux sociaux dirigent leurs activités vers des consommateurs qui ont leur résidence habituelle en Belgique, le consommateur peut toujours recourir aux règles belges en matière de clauses abusives si celles-ci offrent une plus grande protection. De plus, la Commission confirme que, lors de la création d'un profil de réseau social, il est question d'un « contrat » (s'il y a consentement pour s'engager à fournir des prestations qui permettent au consommateur de créer et d'entretenir un réseau social ainsi que d'échanger des informations avec d'autres) entre une « entreprise » (le prestataire est une personne qui poursuit de manière durable un but économique) et un « consommateur » (toute personne physique qui agit à des fins qui n'entrent pas dans le cadre de son activité commerciale, industrielle, artisanale ou libérale ; art. I.2° CDE)[18]. La Commission souligne le fait que le service soit offert « gratuitement » n'est pas important pour l'application des règles en matière de clauses abusives. Elle juge en outre que les contrats ont effectivement été conclus à titre onéreux puisque chaque partie a l'obligation de fournir une prestation. Non seulement les données à caractère personnel des utilisateurs ont une valeur commerciale qui n'est pas à sous-estimer puisqu'elles permettent la diffusion de publicité ciblée, mais encore les prestataires de services négocient généralement le transfert et le droit d'utilisation, à leur avantage, du contenu que l'utilisateur place sur le site de réseau social.

Dans son avis, la Commission examine en outre le rapport entre la législation vie privée et la législation sur les clauses abusives, puisque plusieurs des clauses examinées dans les contrats entre les sites de réseaux sociaux et leurs utilisateurs concernent le traitement des données à caractère personnel. Dans ce contexte, la Commission conclut que la législation vie privée n'exclut pas l'application des dispositions sur les clauses abusives, que les clauses contractuelles qui ignorent la législation vie privée sont abusives et que les clauses concernant l'objet et le prix ne peuvent jamais se rapporter à quelque chose d'« illégal ».

[16] Disponible à l'adresse http://economie.fgov.be/fr/binaries/CCA38_tcm326-276733.pdf.
[17] http://economie.fgov.be/fr/spf/structure/Commissions_Conseils/Commission_clauses_abu/#.VxSktpN97rc.
[18] La Commission souligne le fait que les utilisateurs qui adhèrent au réseau social à des fins promotionnelles ou pour entretenir un réseau professionnel, n'agissent pas comme consommateurs.

L'examen des conditions d'utilisation par la Commission a dressé un aperçu des clauses les plus problématiques et les plus discutables au vu de la nature particulière de la fourniture du « service de réseau social ». Dans la mesure où l'analyse de ces clauses ne peut être examinée en détail dans le cadre de l'ampleur limitée du présent rapport, nous nous limitons à l'énumération de quelques points cruciaux à propos desquels la Commission formule des recommandations en conclusion de son avis : 1) les exigences de clarté et d'intelligibilité dans le chef du consommateur (« *informed consent* »), 2) les clauses sur le consentement en rapport avec l'utilisation de données personnelles et de données protégées par le droit d'auteur, 3) la modification unilatérale des caractéristiques du service, des conditions, et le droit à la résiliation unilatérale, 4) les limitations de responsabilité et clauses d'exonération de garantie, 5) la compétence judiciaire et les clauses de règlement des litiges, 5) droit applicable. En ce qui concerne ce dernier point, la Commission souligne le fait que les clauses qui déclarent d'application des règles de droit étrangères sont non seulement contraires à l'art. VI.84 §2 CDE et à l'art. 6 du Règlement Rome I (supra), mais aussi que ces clauses trompent le consommateur à propos de ses droits légaux, ce qui est contraire à l'exigence de transparence et peut en soi être considéré comme des clauses abusives aux termes de l'art. I.8.22° CDE.[19]

III / Mondialisation, Internet et les difficultés de la répression des pratiques illicites

A) Pédopornographie sur Internet

La législation belge lutte contre la pédopornographie par l'article 383*bis* C.pén. Cet article est formulé de façon neutre en termes technologiques, car au moment de son introduction en 1995, il a été fait abstraction du média. Il ne fait dès lors aucun doute que l'article 383*bis* C.pén. s'applique également à la pédopornographie *en ligne*. Il est important de savoir que le producteur ou le distributeur de matériel pédopornographique ne sont pas les seuls susceptibles d'être sanctionnés, le possesseur peut également l'être. La Cour de cassation a précisé en outre en 2011 que « *la possession d'images à caractère pornographique impliquant ou présentant des mineurs, qui est punie par la loi, ne requiert pas que l'utilisateur d'un ordinateur manifeste sa maîtrise d'une image par le téléchargement ou l'impression de celle-ci ni qu'il la détienne de manière continue. Le seul fait d'accéder à un site informatique et de visionner les images, en connaissance de cause, suffit* ».[20] Fin 2011, la possession et l'accès *« en connaissance de cause, par un système informatique ou par tout moyen technologique »* à du matériel pédopornographique ont été ajoutés aux faits punissables. La formulation de l'article 383*bis* C.pén. (« *ou présentant des mineurs* ») permet de déduire que la pédopornographie virtuelle (dans lesquelles aucun enfant n'est impliqué mais dont les images de mineurs utilisées sont générées par ordinateur) entrent dans le champ d'application de cet article.

B) Racisme sur Internet

[19] Art. I.8.22° CDE: clause abusive : *« toute clause ou toute condition dans un contrat entre une entreprise ou une personne exerçant une profession libérale et un consommateur qui, à elle seule ou combinée avec une ou plusieurs autres clauses ou conditions, crée un déséquilibre manifeste entre les droits et les obligations des parties au détriment du consommateur ».*

[20] Cass. 20 avril 2011 ; voir également Cass. 26 octobre 2011 ; Corr. Tongres, le 25 octobre 2012, *Limb.Rechtsl.* 2013, 1, 47.

Les discours racistes tenus sur Internet sont susceptibles d'être punis en vertu de la loi du 30 juillet 1981 tendant à réprimer certains actes inspirés par le racisme ou la xénophobie (loi contre le racisme). Par essence, trois types de discours racistes sont sanctionnés : l'art. 20 rend passible de sanctions pénales l'incitation à la discrimination, la ségrégation, la haine ou la violence à l'égard d'une personne, d'un groupe, d'une communauté ou de leurs membres, fondée sur la nationalité, une prétendue race, la couleur de peau, l'ascendance ou l'origine nationale ou ethnique, l'art. 21 concerne la diffusion publique d'idées fondées sur la supériorité ou la haine raciale, et l'art. 22 rend passible de sanctions pénales l'appartenance ou la participation à un groupement ou une association qui, de manière publique, manifeste et répétée, prône la discrimination ou la ségrégation fondée sur l'un des critères mentionné ci-avant. Ce que l'on entend par « public » est défini à l'art. 444 C.pén. : *« soit dans des réunions ou lieux publics (alinéa 1) ; soit en présence de plusieurs individus, dans un lieu non public, mais ouvert à un certain nombre de personnes ayant le droit de s'y assembler ou de le fréquenter (alinéa 2) ; soit dans un lieu quelconque, en présence de la personne offensée et devant témoins (alinéa 3) ; soit par des écrits imprimés ou non, des images ou des emblèmes affichés, distribués ou vendus, mis en vente ou exposés aux regards du public (alinéa 4) ; soit enfin par des écrits non rendus publics, mais adressés ou communiqués à plusieurs personnes (alinéa 5)* ». Cette énumération date de l'époque pré-Internet, mais elle peut être interprétée de façon évolutive. Ainsi, un site Internet accessible à tous peut être assimilé à un lieu public, et un profil de réseau social exclusivement accessible par un nombre limité d'« amis » à la situation décrite à l'alinéa 2. Un jugement du 22 décembre 1999 estimait que des discours racistes tenus sur Internet, *in casu* un groupe de discussion en ligne, entrent dans le champ d'application de la loi contre le racisme.[21] Cela a été confirmé à plusieurs reprises.[22]

La victime ou le Ministère public ne sont pas les seuls à pouvoir initier des poursuites pénales. Des associations telles que la Ligue des droits de l'homme, le Mouvement contre le Racisme, Antisémitisme et la Xénophobie, ou Unia (art. 31, 32 et 33 de la loi contre le racisme). Comme indiqué précédemment, depuis 1999, les délits de presse inspirés par le racisme et la xénophobie sont traités par les tribunaux correctionnels.

Dans ce contexte, citons encore la loi du 23 mars 1995 tendant à réprimer la négation, la minimisation, la justification ou l'approbation du génocide commis par le régime national-socialiste allemand pendant la seconde guerre mondiale (la loi sur le négationnisme), la loi du 10 mai 2007 tendant à lutter contre certaines formes de discrimination,[23] la loi du 10 mai 2007 tendant à lutter contre la discrimination entre les femmes et les hommes, et la loi du 22 mai 2014 tendant à lutter contre le sexisme dans l'espace public. Toutes ces lois s'appliquent également aux discours sur Internet.[24]

C) Transfert des données par les acteurs d'Internet aux autorités nationales

[21] Corr. Bruxelles, le 22 décembre 1999, *Auteurs & Media* 2000, 1-2, 134, note Dirk Voorhoof.
[22] Par exemple : Bruxelles, 23 janvier 2009, *Auteurs & Media* 2009, 6, 639, Trib. Bruxelles, le 27 novembre 2009.
[23] Les motifs de discrimination retenus dans la loi générale anti-discrimination sont les suivants : âge, orientation sexuelle, état civil, naissance, fortune, convictions religieuses ou philosophiques, convictions politiques, convictions syndicales, langue, état de santé actuel ou futur, handicap, caractéristique physique ou génétique ou origine sociale (art. 3).
[24] Pour ce qui est de l'application de la loi sur le négationnisme aux discours diffusés par le biais d'un site web : Corr. Bruxelles, le 23 juin 2015, www.unia.be.

En vertu de l'art. 46bis du Code d'instruction criminelle (C.instr.crim.), le Procureur du Roi[25] peut, en recherchant les crimes et les délits, requérir le concours de l'opérateur d'un réseau de communication électronique ou d'un fournisseur d'un service de communication électronique, concernant 1° l'identification de l'abonné ou de l'utilisateur habituel d'un service de communication électronique ou du moyen de communication électronique utilisé ou 2° l'identification des services de communication électronique auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée. Ces données peuvent par exemple porter sur l'identification des expéditeurs d'e-mails anonymes, des utilisateurs anonymes de chatbox ou de réseaux peer-to-peer et des utilisateurs d'adresses IP.[26] Après des années de procédure judiciaire dans « l'affaire Yahoo », en décembre 2015, la Cour de cassation a confirmé que la collaboration en vertu de l'art. 46bis peut être demandée à tout opérateur ou fournisseur qui dirige ses activités économiques sur les consommateurs en Belgique, même lorsqu'il est établi à l'étranger (*in casu* Yahoo, établie aux États-Unis).[27]

IV/ Mondialisation, Internet et les nouvelles opportunités

A) Jeux en ligne

Aux termes de la loi du 7 mai 1999 sur les jeux de hasard, les paris, les établissements de jeux de hasard et la protection des joueurs, les jeux de hasard[28] via « des instruments de la société de l'information »[29] ne sont autorisés que moyennant l'octroi par la Commission des jeux de hasard d'une licence supplémentaire (art. 43/8). Il a été décidé de recourir à un système de licences supplémentaire. Cela implique qu'une licence pour des « jeux de hasard en ligne » peut exclusivement être accordée à des établissements qui disposent déjà d'une licence pour l'exploitation de jeux de même nature que ceux offerts dans le monde « réel ». La Commission des jeux de hasard publie sur son site web une liste noire des sites de jeux de hasard illégaux.[30] Les personnes qui jouent sur l'un de ces sites web sont passibles de sanctions pénales (art. 4, §2 et art. 64). La Belgique a instauré un climat fiscal favorable à l'offre de jeux de hasard en ligne (11 %).[31]

B) "Digital Belgium" et l'économie de partage

En avril 2015, le ministre belge de « l'Agenda numérique » a soumis un plan d'action « Digital Belgium ».[32] Ce plan d'action identifie cinq priorités : 1) infrastructures numériques, 2) confiance dans le numérique et sécurité numérique, 3) économie numérique, 4) pouvoirs

---

[25] En cas d'extrême urgence, chaque officier de police judiciaire peut, avec l'accord oral et préalable du procureur du Roi, et par une décision motivée et écrite requérir ces données.
[26] Jos Dumortier, avec la collaboration de Hans Graux en Frederic Debusseré, ICT-recht, 2013, Acco, 354-355.
[27] Cass. 1er décembre 2015 :
[28] « Un jeu de hasard » est défini à l'art. 2, 1° comme tout jeu pour lequel un enjeu de nature quelconque est engagé, ayant pour conséquence soit la perte de l'enjeu par au moins un des joueurs, soit le gain de quelque nature qu'il soit, au profit d'au moins un des joueurs, ou organisateurs du jeu et pour lequel le hasard est un élément, même accessoire, pour le déroulement du jeu, la détermination du vainqueur ou la fixation du gain.
[29] Par « instruments de la société de l'information », il convient d'entendre : équipements électroniques de traitement, y compris la compression numérique, et de stockage de données, qui sont entièrement transmises, acheminées et reçues par fils, par radio, par des moyens optiques ou par d'autres moyens électromagnétiques (art. 2, 10°).
[30] http://www.gamingcommission.be/opencms/opencms/jhksweb_fr/gamingcommission/news/news_0001.html.
[31] http://finances.belgium.be/sites/default/files/downloads/jeux_et_paris.pdf.
[32] http://www.digitalbelgium.be/.

publics numériques, et 5) compétences et emplois numériques. Dans le contexte de la priorité concernant l'économie numérique, un plan start-up a été proposé pour les start-ups du secteur numérique, assorti d'un tax shelter et d'incitants fiscaux pour le crowdfunding. Les conditions en ont été fixées par le gouvernement fédéral.[33] De plus, l'accent est mis sur le fait que des modèles d'entreprise novateurs, par exemple dans l'économie de partage, doivent pouvoir travailler dans un cadre de sécurité juridique qui permet la croissance.

Dans la pratique, les initiatives de l'économie de partage telles qu'AirBnB (offre de chambres d'hôtes en ligne) se heurtent cependant à des obligations et à des obstacles juridiques. Ainsi, le décret flamand du 5 février 2016 relatif à l'hébergement touristique fixe les conditions qu'il convient de respecter pour exploiter un hébergement touristique. Les personnes qui souhaitent proposer un hébergement touristique, également par le biais de sites web tels qu'AirBnB, devront le signaler au service « Toerisme Vlaanderen ».[34]

Uber, un service de taxi alternatif qui fonctionne par une app sur smartphone, a également déjà fait l'objet de litiges juridiques en Belgique. En septembre 2015, le Tribunal de commerce de Bruxelles a jugé qu'Uber propose effectivement des services de taxi, services qui sont assortis d'obligations par l'Ordonnance de la Région de Bruxelles-Capitale du 27 avril 1995 relative aux services de taxis et aux services de location de voitures avec chauffeur.[35] Le juge a estimé que l'offre de chauffeurs non-rémunérés par Uber est contraire aux pratiques de marché honnêtes. En ce qui concerne la situation où la rémunération obtenue n'excède pas les frais, le juge bruxellois a posé une question préjudicielle à la Cour de justice de l'Union européenne afin de vérifier si dans ce cas, une interdiction serait contraire à la liberté d'entreprendre et à la libre circulation des biens et des services. Dans le courant de l'année 2015, un « Plan taxi » ou un « Plan de transport rémunéré de personnes 2015-2019 » a été proposé au sein du gouvernement bruxellois. L'une de ses priorités est l'adoption d'un nouveau cadre juridique général pour tous les services de transport rémunéré de personnes,[36] mais il n'a actuellement toujours pas été mis en œuvre.

En outre, une initiative a été prise au niveau fédéral, en avril 2016, afin d'introduire un taux d'imposition réduit pour les personnes qui fournissent des services par le biais d'une app ou d'une plate-forme numérique dans l'économie de partage.[37]

---

[33] Cf. http://decroo.belgium.be/fr/le-gouvernement-f%C3%A9d%C3%A9ral-d%C3%A9finit-les-conditions-du-tax-shelter-et-du-crowdfunding-pour-les-start-ups.

[34] Le gouvernement flamand doit encore fixer la date d'entrée en vigueur.

[35] Disponible à l'adresse http://www.legalworld.be/legalworld/uploadedFiles/Rechtspraak/De_Juristenkrant/Kh.%20Brussel%2025%20september%202015%20(UberPop).pdf?LangType=2067.

[36] http://www.pascalsmet.be/media/attachments/15/03/Principenota---Plan-bezoldigd-personenvervoer-2015---2019.pdf.

[37] http://decroo.belgium.be/fr/baisse-des-charges-pour-les-personnes-qui-exercent-une-activit%C3%A9-compl%C3%A9mentaire-dans-l%E2%80%99%C3%A9conomie.