Criminalité informatique

Forget, Catherine; Dumortier, Franck

Published in:
Revue du Droit des Technologies de l'information

Publication date:
2015

Document Version
le PDF de l'éditeur

critère retenu par elle pour déclarer une preuve irrégulière irrecevable, cette cause d'écartement n'a lieu d'être que lorsque la fiabilité est imputable à l'illégalité ou à l'irrégularité de l'acte qui en a permis l'obtention.

Dans un litige tranché par la cour du travail de Liège, division Liège[652], la cour accepte de recevoir comme preuve un enregistrement audio réalisé par un travailleur à l'insu de son employeur du fait qu'aucun des trois critères Antigone n'est rencontré en l'espèce. La cour pointe en particulier que la fiabilité de l'enregistrement audio n'est pas mise en doute – au contraire de sa retranscription, qu'elle écarte.

En sens inverse, la cour du travail de Bruxelles[653] a écarté un enregistrement vidéo réalisé à l'insu de l'employeur, en raison de son manque de fiabilité. Elle met en cause le procédé tout à fait orienté dans la mesure où le but de la manœuvre étant d'obtenir confirmation de ce que l'employeur avait oralement notifié au travailleur son licenciement lors d'une précédente réunion. Du fait que l'entretien a été provoqué avec la possibilité de préparer des questions induisant certaines réponses, la preuve recueillie est jugée non crédible. La cour considère en outre que le procédé est déloyal et porte atteinte au droit à un procès équitable. Elle énonce encore que « le principe de proportionnalité s'oppose à ce que la preuve recueillie illégalement puisse être admise pour établir l'existence d'un congé, soit un acte juridique relative à la résiliation d'une relation contractuelle entre un travailleur et son employeur ».

IV. CRIMINALITÉ INFORMATIQUE

Catherine Forget[654] et Franck Dumortier[655]

209. Introduction. Tant en matière de droit pénal matériel qu'en matière de procédure pénale, la jurisprudence « accessible » qu'examine cette chronique 2012-2014 relative à la criminalité informatique s'est avérée être extrêmement rare[656]. Le lecteur s'étonnera légitimement de cette disette étant donné la richesse de l'actualité dans ce domaine.

Pour ne citer qu'un exemple, le piratage informatique ne cesse de défrayer la chronique : le piratage de Belgacom, de la SNCB, du système des Affaires étrangères belges, du Service public fédéral Économie, du site du ministère wallon de l'Économie, du site d'une zone de la police du Brabant wallon et ceci, sans oublier les nombreux piratages informatiques visant directement des particuliers. Dès lors, force est de constater que, malgré le peu de jurisprudence publiée, la criminalité informatique est un domaine en plein essor.

652 C. trav. Liège (div. Liège, 15e ch.), 20 novembre 2014, R.G. n° 2014/AL/54, www.juridat.be.

653 C. trav. Bruxelles (4e ch.), 7 janvier 2015, R.G. n° 2012/AB/1278, www.juridat.be.

654 Chercheur au CRIDS, avocate au barreau de Bruxelles.

655 Chercheur senior au CRIDS et assitant au Master de spécialisation en droit des TIC.

656 Par la rareté des décisions « accessibles », les auteurs considèrent aussi bien celles ayant été éditées que les décisions inédites référencées par voie doctrinale. De manière assez symptomatique, au niveau du droit pénal matériel, nous n'avons pu trouver aucune décision illustrant les infractions spécifiques de fraude informatique et de sabotage informatique.

Ainsi, le Gouvernement fédéral vient de mettre sur pied un Centre relatif à la cybersécurité (CCB) afin de permettre entre autres d'améliorer la sécurité numérique en Belgique[657]. En outre, le législateur étoffe l'arsenal législatif par de nouvelles lois relatives à la prédation des mineurs effectuée par le biais de technologies de la communication et de l'information. Enfin, comme nous le verrons, les cours et tribunaux adoptent parfois des positions surprenantes en matière de procédure pénale liée aux nouvelles technologies.

A. Droit matériel

1. Faux en informatique

210. Principe. Le faux informatique requiert une altération de la vérité par l'introduction, la modification ou l'effacement de données qui sont stockées, traitées ou transmises par un système informatique ou par la modification, par tout moyen technologique, de l'utilisation possible des données dans un système informatique[658].

211. Annonce de vente en ligne sous un faux nom. Le 3 octobre 2013, la cour d'appel d'Anvers s'est penchée sur l'insertion, sur le site web eBay, d'une annonce mettant en vente des consoles de jeux sous un faux nom dans le but frauduleux d'obtenir de l'argent sans intention de livrer les biens vendus[659]. Sur son compte d'utilisatrice, outre un faux nom, la prévenue avait également mentionné une adresse fictive ainsi qu'un numéro de téléphone renvoyant à une cabine publique ; seul le compte bancaire de cette dernière y était référencé de manière exacte. En première instance, ces faits avaient été qualifiés de *crimes* de faux et usage de faux en écritures privées incriminés par l'article 196 du Code pénal. Dans son arrêt, la cour d'appel d'Anvers les requalifie de *délits* de faux et usage de faux en informatique au sens de l'article 210*bis* du Code pénal[660]. Cette requalification de la cour d'appel d'Anvers suit la logique de la *ratio legis* de l'article 210*bis* du Code pénal qui a précisément été inséré dans le Code pénal par la loi du 28 novembre 2000[661] pour mettre un terme aux contestations juridiques sur la question de savoir si les données électroniques peuvent être rangées parmi les écritures et donc protégées par les dispositions pénales classiques en matière de faux en écritures[662]. Relevons par ailleurs que la vente en ligne, ayant été réalisée suite à cette annonce, a également été qualifiée par la cour d'appel d'Anvers d'escroquerie de droit commun visée à l'article 496 du Code pénal[663].

212. Usurpation d'identité sur un forum internet. Dans son arrêt du 21 juin 2012, la cour d'appel de Gand eut à se prononcer sur la qualification des faits suivants : le prévenu avait fait

657 A.R. du 10 octobre 2014 portant création du Centre pour la Cybersécurité Belgique, *M.B.*, 21 novembre 2014.

658 Art. 210*bis* du Code pénal. Comme pour le faux en écritures de droit commun, il est requis que les données manipulées aient une portée juridique. À ce sujet, voy. O. Leroux, « Criminalité informatique », in *Les infractions contre les biens*, Bruxelles, Larcier, 2008, p. 388. Pour une étude approfondie de cette incrimination, voy. O. Leroux, « Le faux informatique », *J.T.*, 2004, pp. 509 et s.

659 Anvers, 3 octobre 2013, *N.C.*, 2014/5, pp. 418-420.

660 Pour une analyse comparative des infractions incriminées respectivement par les articles 196 et 210*bis* du Code pénal, voy. C. Conings, « Faux réel *vs.* faux virtuel », *NjW*, 2013/6, n° 279, pp. 238-243.

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

662 Sur ce point, voy. O. Leroux, « Criminalité informatique », *op. cit.*, p. 382.

663 Et non, et à raison, de fraude en informatique visée par l'article 504*quater* du Code pénal ; l'élément matériel de cette infraction consistant en la recherche d'un avantage illicite par la tromperie d'une machine – et non d'une personne –, ce qui n'est pas le cas dans cette affaire. À ce sujet, voy. O. Leroux, « Criminalité informatique », *op. cit.*, p. 402.

l'aveu d'avoir utilisé un prénom et un nom fictifs (« P.D. ») ainsi que son propre numéro de GSM sur un forum internet afin de s'identifier pour répondre au message d'un participant[664]. Dans cette affaire, la cour fit usage de l'article 231 du Code pénal qui incrimine le fait, pour un individu, de porter publiquement un nom[665] qui ne lui appartient pas[666]. En l'espèce, la cour estima la condition de publicité remplie[667]. Elle jugea également que l'article 231 du Code pénal n'exige pas que l'auteur des faits ait eu la volonté de cacher son identité ; il suffit qu'il ait eu la volonté de faire croire ou de laisser croire que le faux nom était véritablement le sien. Notons, pour le surplus, que pour des faits similaires, certaines juridictions ont parfois opté, pour la qualification de faux en informatique au sens de l'article 210*bis* du Code pénal, en sus de celle de port public de faux nom, lorsque la portée juridique de données a été modifiée[668].

213. Port de faux nom sur un réseau social[669]. Dans cette affaire jugée par le tribunal correctionnel de Bruxelles, les prévenus avaient mené une enquête pour démontrer qu'une personnalité politique était toujours active dans un mouvement d'extrême droite, malgré les démentis officiels de celle-ci[670]. Pour parvenir à leurs objectifs, les prévenus avaient créé, sur Facebook, un profil au nom d'une personne inexistante de sexe féminin affichant des opinions proches de celles de l'extrême droite. Ils s'étaient contenté de laisser exister ce profil passivement, sans envoyer aucune invitation à qui que ce soit, afin d'observer si ce profil serait contacté d'initiative par des militants d'extrême droite. La personnalité ciblée aurait alors elle-même établi un premier contact via le site de rencontre *Badoo*, à la suite duquel les prévenus avaient adressé à cette dernière une demande d'amitié via le profil Facebook susmentionné. Via Facebook, les protagonistes auraient ensuite procédé à des échanges de messages pendant une dizaine de jours, au cours desquels la personnalité ciblée dévoila la poursuite de ses activités politiques au sein de l'extrême droite. Le tribunal qualifia ces faits de port public de faux nom, au sens de l'article 231 du Code pénal, rejetant l'argument des prévenus selon lequel le profil Facebook avait été créé « au nom » d'un pseudonyme. Selon le tribunal, l'usage d'un pseudonyme sur les réseaux sociaux ne doit « laisser

664 Gand, 21 juin 2012, *R.A.B.G.*, 2013/8, p. 501 (note F. Van Volsem, pp. 501 à 507).

665 Notons que le port public d'un faux prénom n'est pas, en tant que tel, punissable par l'article 231 du Code pénal. Voy. Mons, 29 mai 1996, *R.D.P.C.*, 1997, p. 568 et la référence aux travaux préparatoires ; Bruxelles, 2 décembre 1875, *Pas.*, 1876, II, p. 25.

666 Pour une étude des éléments constitutifs du délit visé à l'article 231 du Code pénal, voy. F. Van Volsem, « L'usage du nom d'autrui ou d'un nom fictif sur Internet peut être constitutif de l'infraction d'usurpation de nom, note sous Gand, 21 juin 2012 », *R.A.B.G.*, 2013/8, pp. 501-507.

667 Le caractère public du port de faux nom est un élément de fait livré à l'appréciation du juge du fond. Ainsi, par exemple, l'utilisation d'un faux nom sur un site de rencontre a déjà été considérée par le passé comme répondant à la condition de publicité. Voy. Bruxelles, 22 juin 2010, R.G. n° 2008BC542, inédit, cité par A. Weyembergh et L. Kennes, *Droit pénal spécial*, t. I, Limal, Anthemis, 2011, p. 241, n° 403.

668 Voy. par ex. Corr. Gand, 21 septembre 2011, *N.C.*, 2014, liv. 1, p. 68, note F. Delbar ; *T. Strafr.*, 2012, liv. 2, p. 103, note E. Baeyens. Dans cette affaire, une employée désireuse de se venger de son ancien employeur qui l'avait licenciée avait créé un faux profil Facebook au nom de celui-ci. Des messages accusant l'employeur d'entretenir des relations adultères avaient ensuite été postés, sur ce profil, à partir de soi-disant « amis » dont les profils avaient également été créés par l'employée. Les faits à charge de la prévenue furent qualifiés, par le tribunal correctionnel de Gand, de faux en informatique ainsi que de port public de faux nom. D'autres exemples sont référencés par M. Giacometti et P. Monville, in M. Salmon (coord.), *Les Réseaux sociaux et le droit*, coll. Collection de la Conférence du Jeune Barreau de Bruxelles, Larcier, Bruxelles, 2014, pp. 179-210.

669 Voy. *infra*, n^os^ 324 et s.

670 Corr. Bruxelles, 20 mai 2014, inédit, cité par M. Giacometti et P. Monville, in M. Salmon (coord.), *Les Réseaux sociaux et le droit*, *op. cit.*, pp. 194-196.

planer aucun doute quant au fait qu'il s'agit d'un pseudonyme parce qu'il s'agit d'un surnom, d'un sobriquet ou d'une référence à un héros cinématographique »[671] et « c'est la personne elle-même qui pour assurer son anonymat ou sa tranquillité choisit de s'attribuer un pseudonyme et non un tiers »[672]. Pour le surplus, le tribunal refusa de qualifier ces faits de faux en informatique, considérant que l'introduction d'un profil fictif sur Facebook et le contenu même des messages envoyés n'entraînent pas une modification de la portée juridique des données[673]. À cet égard, le tribunal précisa que « les données (fictives) introduites sur le réseau social constituent des déclarations relatives à des faits personnels ou à des situations propres, certes inventés mais il faut considérer que ces déclarations sont de pures allégations auxquelles ne s'attache pas la présomption de sincérité »[674].

2. Hacking

214. Principe. L'article 550*bis* du Code pénal distingue deux formes d'accès illégal aux systèmes d'information. Le premier paragraphe de cette disposition incrimine le *hacking interne* – soit le fait d'un individu, disposant d'un droit d'accès sur le système visé, de dépasser les limites de son autorisation avec une intention frauduleuse – tandis que le second paragraphe, dédié au *hacking externe*, rend coupable celui qui, étranger au système visé et sachant qu'il n'y est pas autorisé, accède dans ledit système ou s'y maintient[675].

215. Hacking interne entre collègues. Le 5 novembre 2014, la cour d'appel de Bruxelles eut à connaître d'une affaire dans laquelle une ancienne travailleuse s'était procuré des e-mails – dont elle n'était ni l'expéditrice ni la destinataire – en accédant à la boîte e-mail d'une collègue dans le but de se réserver des preuves contre son ex-employeur[676]. L'employeur avait porté plainte au pénal, estimant que la travailleuse avait commis un *hacking interne* pour se procurer ces courriers électroniques afin de les produire en justice. La cour considéra l'élément matériel du délit visé à l'article 550*bis*, § 2, du Code pénal établi dès lors que ladite travailleuse avait outrepassé son pouvoir d'accès en accédant à la boîte e-mail de sa collègue sans autorisation. Les faits révélaient que la collègue en question laissait sa messagerie électronique ouverte en permanence, même

671 Par cette décision, le tribunal confirme que le nom protégé pris ne doit pas nécessairement être celui d'une autre personne existante mais qu'il peut également s'agir d'un nom purement fictif. Voy. I. Delbrouck, « Nom, port du nom et faux nom », in X., *Postal Mémorialis. Lexique du droit pénal et des lois spéciales*, juin 2013, n° 50/25.

672 Cette remarque rappelle le droit d'un utilisateur d'un réseau social de faire usage d'un pseudonyme lors de la création de son profil. Cette technique permet d'une part de protéger l'individu du droit à la vie privée en ligne afin de pouvoir exercer, de manière anonyme sa liberté d'expression.

673 La modification de la portée juridique des données est une condition nécessaire de l'incrimination, de faux en informatique qui doit être constatée *in concreto* par le juge du fond. La portée réelle de cette notion de « modification de la portée juridique des données » semble toutefois difficile à définir avec précision. Toutefois, dans l'exposé des motifs, on peut lire que cette condition peut être « considérée comme la réalisation effective d'un inconvénient spécifique ». Sur ce point, voy. O. Leroux, « Le faux informatique », *op. cit.*, p. 513.

674 On peut s'étonner de la contradiction de cette assertion du tribunal avec le motif qui amène celui-ci à considérer l'élément moral de l'infraction de port public de faux nom établi, à savoir l'intention générale de porter le faux nom pour faire croire qu'il s'agit du véritable nom. Le tribunal semble ici faire une application « deux poids, deux mesures » d'une apparente sincérité selon la qualification examinée.

675 Pour une étude des éléments constitutifs de ces deux formes de hacking, voy. O. Leroux, « Criminalité informatique », *op. cit.*, pp. 410 et s.

676 Bruxelles (14e ch.), 5 novembre 2014, R.G. n° 2013/CO/177, inédit, cité par K. Rosier, « Un hacking entre collègues condamné au pénal », *B.J.S.*, n° 540, 2015, p. 15.

lorsque celle-ci quittait la pièce, de sorte que la prévenue avait facilement pu *activement* consulter les e-mails de cette dernière afin de sélectionner et d'imprimer ceux qui l'intéressaient[677]. Quant à l'élément moral de l'infraction, la cour estima l'intention frauduleuse caractérisée dès lors que la prévenue s'était procurée un instrument de preuve auquel elle n'avait pas droit afin d'obtenir la reconnaissance de ses droits, fussent-ils véritables. Le fait, notamment d'imprimer des e-mails auxquels elle n'avait pas un accès autorisé et de les remettre ensuite à son conseil suffisait à démontrer que son but était bien de se constituer frauduleusement un moyen de preuve.

216. Hacking externe entre collègues. Le jugement du tribunal correctionnel d'Anvers du 10 novembre 2014 illustre que la notion d'« accès » à un système d'information – l'élément matériel du hacking – ne requiert pas la réalisation de manipulations informatiques complexes[678]. En l'espèce, à partir du smartphone d'entreprise d'un travailleur que celui-ci avait restitué après sa démission, un employeur avait accédé à un compte de messagerie électronique personnel et non sécurisé y installé par le travailleur. Un simple toucher sur l'écran tactile du smartphone avait permis à l'employeur de s'introduire, via son propre système informatique (le smartphone), dans un système informatique qui ne lui appartient pas (le compte de messagerie électronique du travailleur)[679]. Le tribunal considéra ces circonstances comme étant suffisantes pour établir l'élément matériel du *hacking externe*. Quant à l'élément moral, le juge estima celui-ci établi dès lors que des courriers électroniques du compte piraté avaient été transférés par l'employeur vers son propre compte e-mail. Pour le surplus, il était démontré à suffisance qu'il existait un lien intrinsèque entre l'infraction et les intérêts de la personne morale étant donné que les courriers transférés concernaient le personnel, les clients et les fournisseurs de la société et que ces courriels avaient été utilisés par cette personne morale dans le cadre d'une procédure judiciaire.

3. Harcèlement et technologies de la communication

217. La diffusion d'une vidéo sur YouTube peut être constitutive de harcèlement au sens du droit commun[680]. L'article 442*bis*, alinéa 1er, du Code pénal incrimine quiconque porte gravement atteinte, par des agissements incessants ou répétitifs, à l'environnement personnel d'autrui en l'importunant de manière irritante. Ces agissements pour être constitutifs de harcèlement ne sont en principe pas isolés[681]. Dans un arrêt du 29 octobre 2013[682], la Cour de cassation considère que la diffusion de vidéos sur internet, en l'espèce sur YouTube, peut mener au harcèlement d'une

677 Relevons à cet égard que la cour releva qu'en l'espèce, il ne s'agissait pas d'une prise de connaissance accidentelle d'une démarche active. En effet, la simple consultation passive d'un contenu apparaissant à l'écran n'est pas punie par l'article 550*bis*, la notion d'accès supposant, selon O. Leroux, « un acte positif (*modus operis*) traduisant avec certitude la volonté de l'agent de pénétrer d'une quelconque façon dans le système informatique convoité » (voy. O. Leroux, « Criminalité informatique », *op. cit.*, p. 413).

678 Corr. Anvers, 10 novembre 2014, *T. Strafr.*, 2015/2, p. 96 (note G.S., « Het misdrijf van externe hacking », p. 96).

679 Relevons que l'élément matériel du hacking externe ne requiert pas d'outrepasser un quelconque système de sécurité, la seule exigence étant d'accéder ou de se maintenir dans un système informatique en l'absence totale d'autorisation. Voy. O. Leroux, « Criminalité informatique », *op. cit.*, p. 411.

680 Voy. *infra*, n° 317.

681 À cet égard voy. M. De Rue, « Le harcèlement », in H.-D. Bosly et C. De Valkeneer (dir.,) *Les infractions*, vol. 2, *Les infractions contre les personnes*, Bruxelles, Larcier, 2010, pp. 731-733.

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

personne, l'acte initial fut-il unique et non répété[683]. Selon la Cour, l'auteur devait connaître les conséquences de son comportement, à savoir des insultes et commentaires affectant la tranquillité des personnes de manière quasi permanente durant une période continue. La Cour relève en effet que « le propre d'internet en général et de forums ou sites internet tels que You Tube en particulier est que des vidéos et commentaires qui y sont postés peuvent être entendus ou vus de manière permanente par un nombre incalculable de personnes ». Il n'est donc pas requis que la victime ait regardé la vidéo une ou plusieurs fois, il suffit que cette vidéo soit accessible à une quantité importante de personnes[684]. La Cour fonde son appréciation sur la nature de l'acte initial et les conséquences de celui-ci à l'égard de la victime, en l'occurrence, la personne visée initialement mais aussi à l'égard de toute personne affectée par le comportement de l'auteur, à savoir les proches de celle-ci[685]. En tout état de cause, la Cour souligne qu'il revient au juge du fond d'apprécier *in concreto* si la tranquillité de la personne est gravement affectée pour examiner la prévention de harcèlement de droit commun.

Notons que le harcèlement au sens de l'article 442*bis* du Code pénal se distingue du harcèlement réalisé par le biais d'un réseau ou d'un service de communications électroniques au sens de l'article 145, § 3*bis*, de la loi du 13 juin 2005 relative aux communications électroniques[686]. L'article précité incrimine quiconque « 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 celle-ci »[687]. À la différence du harcèlement de droit commun, premièrement, le harcèlement au moyen de communications électroniques ou plus correctement nommé « l'usage abusif de communications électroniques »[688] requiert un contact entre l'auteur et la victime, cette dernière devant être son correspondant et non un tiers quelconque[689]. Deuxièmement, l'usage abusif de communications électroniques ne requiert pas une plainte de la prétendue victime pour entamer les poursuites[690].

683 La Cour de cassation est également amenée à se prononcer sur la qualification des vidéos litigieuses diffusées sur internet en « délit de presse ». La Cour dit pour droit que les propos tenus par l'intermédiaire d'une vidéo ne relèvent pas du champ d'application de l'article 150 de la Constitution et ne sont donc pas qualifiés de délit de presse. À cet égard voy. 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, pp. 393-397.

684 *Ibid.*, pp. 396.

685 K. Rosier, « Quand poster une vidéo sur internet est constitutif de harcèlement », *B.S.J.*, n° 531, 2014, p. 11.

686 *M.B.*, 20 juin 2005.

687 Pour une étude approfondie de la disposition, voy. not. N. Banneux et L. Kerzmann, « Le mal nommé "harcèlement téléphonique" : chronique des tribulations législatives d'une infraction moderne », *R.D.T.I.*, 2009, n° 34, pp. 29-45.

688 Notons que selon O. Leroux, il est réducteur de qualifier cette disposition de harcèlement considérant que la loi ne requiert pas la répétition du comportement incriminé. Voy. O. Leroux, « Protection pénale des mineurs sur Internet : harcèlement, "Grooming" et cyberprédation », in J.-F. Henrotte et F. Jongen (dir.), *Pas de droit sans technologie*, Bruxelles, Larcier, 2015, p. 222.

689 Voy. O. Leroux, « Criminalité informatique », in X., *Postal Mémorialis. Lexique du droit pénal et des lois spéciales*, juillet 2014, C 362/38, p. 50.

690 En effet, l'article 442*bis*, alinéa 2, du Code pénal précise que le harcèlement de droit commun est un délit sur plainte et ne peut être poursuivi que sur plainte de la prétendue victime.

4. La prédation sur internet

218. Corruption de la jeunesse sur internet. Le fait d'entrer en contact sur un *chat* avec une mineure d'âge et de lui proposer d'avoir des relations sexuelles contre rémunération par le biais d'un faux nom et d'une fausse adresse de courrier électronique peut constituer, d'une part, un faux en informatique et, d'autre part, une incitation à la débauche au sens de l'article 379 du Code pénal[691]. Cette infraction serait aujourd'hui qualifiée de « cyberprédation » au sens de l'article 433*bis*/1 du Code pénal.

219. Modification législative. Désormais, les lois du 10 avril 2014[692] insèrent respectivement aux articles 377*ter*, 377*quater* et 433*bis*/1 du Code pénal les infractions de « grooming »[693] et de cyberprédation[694]. Ces dernières se caractérisent par la criminalisation de comportements dans la phase préparatoire d'infractions de droit commun à savoir l'échange de communications et la manipulation[695]. La première suppose la proposition d'une rencontre par l'intermédiaire des technologies de l'information et la communication entre une personne majeure et une personne de moins de 16 ans accompli. Cette proposition doit être émise en vue de commettre une infraction déterminée aux chapitres V, VI et VII du titre VII du livre II du Code pénal. Enfin, l'article 377*quater* du Code pénal suppose que la proposition soit suivie d'actes matériels menant à la rencontre[696]. Précisons que l'article 377*ter* du Code pénal prévoit une circonstance aggravante subjective dans le cas où le « grooming » est précédé de sollicitations ayant entraîné un affaiblissement des mécanismes de défense du mineur[697].

220. La seconde infraction, à savoir la cyberprédation est prescrite en termes plus larges. L'auteur ne doit pas être animé de l'intention de commettre une infraction à caractère sexuel. La communication doit être effectuée par le biais d'une technologie de l'information et de la communication entre une personne majeure et une personne mineure de moins de 16 ans

691 Cass. (2e ch.), 12 février 2013, R.G. n° P.12.1746.N, www.cass.be. Voy. également L. Stevens, « Le grooming via *internet* », note sous Cass., 12 février 2013, *T.J.K.*, 2013/3, pp. 288-294.

692 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, pp. 35484-35485 et la loi du 10 avril 2014 modifiant le Code pénal en vue de protéger les enfants contre les cyberprédateurs, *M.B.*, 30 avril 2014, p. 35486.

693 Le phénomène de « grooming » est aussi appelé « sollicitation en ligne ». Cela consiste, pour des adultes, à approcher des enfants sur Internet dans le but de gagner leur confiance et de leur causer du tort (par exemple en l'amenant à poser des actes de nature sexuelle).

694 Pour des premiers commentaires, voy. L. Claus, « Cyberkinderlokkerij en *grooming* : daadkrachtig wetgevend optreden of een kwestie van overregulering? », *N.C.*, 2015, pp. 15-24 ; C. Conings, K. De Schepper, « Grooming en cyberkinderlokkerij strafbaar », *Computerr.*, 2014, n° 269, p. 270 ; O. Leroux, « Protection pénale des mineurs sur Internet : harcèlement, "Grooming" et cyberprédation », *op. cit.*, pp. 219-249 ; L. Stevens, « Grooming en cyberlokking strafbaar. Uitbreiding van de strafrechtelijke bescherming van de seksuele integriteit van de minderjarigen in cyberspace », *R.W.*, 2014-2015, n° 22, pp. 844-855 ; K. Rosier, « Renforcement de la lutte contre la cyberprédation », *B.S.J.*, 2014/522, p. 14.

695 O. Leroux, « Protection pénale des mineurs sur Internet : harcèlement, "Grooming" et cyberprédation », *op. cit.*, p. 227.

696 Notons que l'infraction de « grooming » s'inspire directement de dispositions internationales notamment la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels, 25 octobre 2007, CETS, n° 201, dite « Convention de Lanzarote » ratifiée par la Belgique le 7 février 2012 et entrée en vigueur le 1er juillet 2013, et la directive 2011/93/UE du Parlement Européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants ainsi que la pédopornographie, *J.O.U.E.* L 335/1. À cet égard, voy. O. Leroux, « Protection pénale des mineurs sur Internet : harcèlement, "Grooming" et cyberprédation », *op. cit.*, pp. 238 et s.

697 *Ibid.*, pp. 239-240.

supposés ou avérés. L'échange de communications ne doit pas nécessairement être suivi d'une rencontre. Enfin, l'auteur doit, selon l'article 433*bis*/1 du Code pénal, avoir « en vue de faciliter la perpétration à son égard d'un crime ou d'un délit 1° 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 législateur incrimine donc le fait d'user de moyens frauduleux en vue de commettre une infraction à l'égard d'un mineur (réel ou supposé)[698].

5. Incitation à la haine et discrimination

221. Incitation à la haine et discrimination par le biais de vidéos diffusées sur YouTube. Dans un arrêt du 6 juin 2013,[699] la cour d'appel d'Anvers condamne F. Belkacem appartenant à l'organisation Sharia4Belgium du chef de harcèlement au sens de l'article 442*bis* du Code pénal mais aussi du chef de diffamation, d'incitation à la discrimination sur la base de la croyance et d'incitation à la discrimination, à la ségrégation, à la haine ou à la violence à l'égard du groupe des non-musulmans[700]. L'auteur était poursuivi pour avoir tenu des propos grossiers et blessants envers une autre personne par le biais de plusieurs vidéos diffusées sur YouTube. La personne visée était une personnalité politique atteinte d'une maladie incurable. D'autres personnes appartenant également au monde politique étaient également visées ainsi que des non-musulmans.

B. Questions de procédure

1. Saisie de données informatiques et recherche de données informatiques

222. Saisie de données informatiques et recherche de données informatiques. Dans un arrêt du 19 décembre 2014[701], la cour d'appel de Bruxelles tranche certains points de controverses relatifs à la saisie de données informatiques et la recherche de données informatiques. En l'espèce, les services de polices avaient consulté les données stockées dans un ordinateur sans disposer de l'ordonnance d'un juge d'instruction. Or, selon les appelants, la consultation des données stockées est une recherche de données informatiques au sens de l'article 88*ter* C.I.Cr. et relève dès lors de la compétence du juge d'instruction. La cour ne souscrit toutefois pas aux arguments présentés. Selon la cour d'appel, la recherche de données informatiques au sens de l'article 88*ter* C.I.Cr. « ne s'applique pas à la recherche menée directement dans un tel système informatique. Elles ne concernent en effet que l'hypothèse où « cette recherche (est) étendue vers un système informatique (…) ». Selon les juges d'appel, l'exploitation des données stockées dans un système informatique tomberait dans le champ d'application de la saisie de données informatiques au sens de l'article 39*bis* C.I.Cr. et peut dès lors s'effectuer dès le stade de l'information. Cet arrêt mérite certains éclaircissements.

Premièrement, la cour étend les pouvoirs des enquêteurs au stade de l'information dans le cadre de la saisie de données informatiques. Ces derniers peuvent désormais exploiter les données stockées dans un système informatique, en l'occurrence un ordinateur, sans l'intervention d'un

698 Pour un approfondissement voy. *ibid.*, pp. 241-247.
699 Anvers, 6 juin 2013, inédit, disponible à l'adresse suivante : www.diversite.be/jurisprudence.
700 Art. 22 de la loi du 10 mai 2007 tendant à lutter contre certaines formes de discrimination, *M.B.*, 30 mai 2007.
701 Bruxelles (12e ch.), 19 décembre 2014, inédit.

juge d'instruction[702]. Pourtant, l'article 39*bis*, § 2, C.I.Cr. permet au procureur du Roi de saisir les données uniquement « lorsqu'il les découvre ». Cet article ne confère pas pour autant aux enquêteurs le pouvoir d'effectuer une recherche dans le système visé sans l'intervention d'un magistrat[703]. Deuxièmement, la cour ne distingue plus les notions de recherche et d'extension de recherche de données informatiques. Selon la cour, l'article 88*ter* C.I.Cr. viserait uniquement l'extension de la recherche. Toutefois, en reprenant les termes du législateur, la distinction susmentionnée s'impose en vertu de l'obligation de localiser préalablement le système faisant l'objet d'une recherche de données informatiques empêchant tout *hacking* externe des enquêteurs[704]. Le législateur constatant l'importance des systèmes en réseaux, permet d'étendre la recherche de données informatiques à d'autres systèmes[705]. La différenciation entre les deux notions n'est donc pas dénuée de fondement. Force est de constater que la cour d'appel de Bruxelles, en ne distinguant plus l'extension de la recherche de la recherche de données informatiques *stricto sensu*, vide partiellement l'article 88*ter* C.I.Cr. de son contenu. De plus, sur la base d'une définition très large de la saisie de données informatiques, la cour assouplit les conditions pour exploiter un système informatique légalement saisi, celui-ci étant désormais consultable dès le stade de l'information. Cet arrêt est toujours pendant devant la Cour de cassation, une occasion éventuelle pour cette dernière de revoir sa copie[706]. En effet, cet argumentaire a une incidence certaine sur les droits fondamentaux et en particulier, sur les garanties prévues en cas d'ingérence dans le droit à la vie privée. La consultation des données stockées dans un système informatique peut s'avérer particulièrement intrusive de sorte que, selon certains auteurs, un rapprochement peut être effectué entre mesure de perquisition et l'exploitation de données stockées dans un système informatique. Cette analogie traduit l'importance de l'ingérence dans la vie privée d'une personne et la nécessité de prévoir des garanties suffisantes[707]. En outre, cette interprétation porte à mal le

[702] Notons que selon certains auteurs, cette interprétation rejoint l'analyse déjà développée par la Cour de cassation selon laquelle les enquêteurs peuvent se saisir de données téléphoniques, de messages stockés dans un répondeur téléphonique dans le cadre d'une visite domiciliaire (Cass., 27 octobre 1999, *J.T.*, 2000, p. 522). À cet égard, voy. J. De Codt, *Des nullités de l'instruction et du jugement*, Bruxelles, Larcier, 2006, p. 51 ; F. Lugentz, D. Vandermeersch, « Chapitre 2 – Les choses susceptibles d'être saisies », in *Saisie et confiscation en matière pénale*, Bruxelles, Bruylant, 2015, p. 140.

[703] En ce sens, voy. L. Kennes, « Les actes de recherche de la preuve et les modes de preuve », in *Manuel de la preuve en matière pénale*, Malines, Kluwer, 2009, p. 238. Notons que la prise de connaissance des données de (télé)communications en « cours de transmission » relève des articles 90*ter* et s. C.I.Cr. À cet égard, voy. E. Lecroart, « La prise de connaissance d'e-mails "en cours de transmission", un parcours sans fin ? », *R.D.T.I.*, 2014/4, n° 57, pp. 19-41 ; C. De Valkeneer, « Les infractions en matière d'écoutes, de prise de connaissance et d'enregistrement de communications et de télécommunications », in H.-D. Bosly et C. De Valkeneer (dir.,) *Les infractions*, vol. 5, *Les infractions contre l'ordre public*, Bruxelles, Larcier, 2013, pp. 399 et s. ; D. Vandermeersch, *Les recherches en matière de téléphonie et de (télé)communications*, Bruxelles, Éditions du Jeune Barreau de Bruxelles, 2006, pp. 49 et s.

[704] *Doc. parl.*, Ch. repr., sess. 1999-2000, n° 50-213/1, p. 23. Notons que le hacking externe est sanctionné par l'article 550*bis* du Code pénal. À cet égard, voy. F. de Villenfagne et S. Dusollier, « La Belgique sort enfin ses armes contre la cybercriminalité : à propos de la loi du 28 novembre 2000 sur la criminalité informatique », *A&M*, n° 1, pp. 60-81.

[705] Les travaux préparatoires précisent en ces termes : « lorsque les systèmes informatiques pour lesquels une recherche semble nécessaire sont dispersés en différents endroits, plusieurs mandats de perquisition ou de saisie doivent être délivrés ». Voy. *Doc. parl.*, Ch. repr., sess. 1999-2000, n° 50-213/1, p. 22.

[706] Dans une affaire similaire, la Cour de cassation a repris l'argumentaire développé par la cour d'appel, voy. Cass., 11 février 2015, R.G. n° P.14.1739.F, www.cass.be. À cet égard, voy. C. Forget, « La collecte de preuves informatiques en matière pénale », in J.-F. Henrotte et F. Jongen (dir.), *Pas de droit sans technologie*, Bruxelles, Larcier, 2015, pp. 260 et s.

[707] Voy. notamment C. Meunier, « La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique », *Rev. dr. pén.*, 2001/7-8, pp. 663-664 ; T. Incalza, « Strafonderzoek in het digitale

principe de procédure pénale selon lequel l'intervention d'un juge d'instruction est requise en cas d'atteintes aux droits et libertés[708].

223. Le blocage de site internet. Dans l'arrêt *PirateBay* du 22 octobre 2013[709], une ordonnance du juge d'instruction prise sur la base des articles 39*bis* et 89 C.I.Cr. imposait aux opérateurs et fournisseurs d'internet de rendre inaccessible l'accès au contenu des sites liés à l'adresse IP du nom de domaine « thepiratebay.org ». La mesure avait pour objectif d'empêcher la poursuite d'actes faisant l'objet d'une infraction mais aussi de garantir la protection d'intérêts civils. Cet arrêt de la Cour de cassation est intéressant à deux égards. Premièrement, l'obligation de collaborer imposée aux opérateurs et fournisseurs était prise sur la base des dispositions relatives à la saisie de données informatiques soit les articles 39*bis* et 89 C.I.Cr. Or, en vertu de l'article 21 de la loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information[710], ces derniers s'ils constatent une éventuelle infraction, ont la possibilité de prendre des mesures dans l'attente d'une décision du procureur du Roi. Ils ne peuvent donc être contraints d'agir. Pourtant, la Cour de cassation dans l'arrêt en cause, se base sur l'article 39*bis*, § 4, C.I.Cr. pour considérer que l'article précité « n'exclut pas que cet ordre soit adressé à des tiers ». Ce faisant, la Cour impose aux fournisseurs et opérateurs de répondre par la positive à la demande du juge d'instruction sur une base légale relative à la saisie de données informatiques. Pourtant, l'article 88*quater* C.I.Cr. prévoit une obligation de collaboration envers les tiers et la Cour aurait pu s'y référer, celle-ci relevant de la compétence du juge d'instruction. La Cour, en décidant d'obliger certains tiers à collaborer sur la base de l'article 39*bis*, § 4, C.I.Cr., étend donc les compétences du procureur du Roi à l'égard des tiers.

Deuxièmement, l'ordonnance imposant le blocage des données avait deux objectifs distincts, à savoir la sauvegarde d'intérêts civils et l'interruption d'actes susceptibles de constituer une infraction. Or, dans le cadre d'une mesure de saisie au sens de l'article 39*bis* C.I.Cr., le blocage des données peut être ordonné par le procureur du Roi si la copie s'avère impossible. Ce blocage permettra de « mettre sous scellées » les données et de les conserver à titre de preuve[711]. Dans le cadre du § 3 de l'article précité, les données peuvent être rendues indisponibles soit parce qu'elles serviront à titre de preuve, l'original doit donc rester intact, soit parce qu'elles portent atteinte à l'ordre public, aux bonnes mœurs, ou qu'elles représentent un danger. Le procureur du Roi pourra interdire l'accès aux données si elles « forment l'objet de l'infraction ou ont été produites par l'infraction et si elles sont contraires à l'ordre public ou aux bonnes mœurs ou constituent un danger pour l'intégrité »[712]. Les finalités de la saisie sont donc très précises. Or, en l'espèce, l'ordonnance du juge d'instruction ne visait pas à éviter la propagation d'un danger ou d'une infraction susceptible de porter atteinte à l'ordre public ou à conserver les données à titre de preuve. La mesure visait tout au plus de faire cesser une potentielle infraction ou de protéger des intérêts civils. Ce faisant,

tijdperk : zoeking en inbeslagneming », *Jura Falc.*, 2010-2011/2, pp. 329-383 ; B. Losdyck, « Les saisies et perquisitions de matériel informatique : les "garde-fous" entourant leur mise-en-œuvre », *R.D.T.I.*, 2013/3, n° 52.

708 Art. 28*ter*, § 1er, C.I.Cr. et art. 56, § 1er, al. 5, C.I.Cr.

709 Cass. (2e ch., sect. nl.), 22 octobre 2013, R.G. n° P.13.0550.N, www. cass.be. Voy. *supra*, n° 30.

710 Depuis lors, les dispositions de la loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information sont reprises dans le Code de droit économique. Voy. loi du 15 décembre 2013, *M.B.*, 14 janvier 2014, p. 1524.

711 C. Meunier, « La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique », *op. cit.*, p. 674.

712 Art. 39*bis*, § 3, C.I.Cr. C'est nous qui soulignons.

la Cour a étendu les modalités de la saisie de données informatiques à une finalité non visée expressément par l'article 39*bis* C.I.Cr.[713]. Or, la saisie de données informatiques est une mesure d'enquête susceptible d'être effectuée dès le stade de l'information. Par conséquent, l'arrêt en cause étend le pouvoir du procureur du Roi dans la mesure où il autorise celui-ci à bloquer un site internet sans l'autorisation d'un magistrat. Une telle disposition susceptible de porter atteinte à la liberté d'expression d'une personne protégée par l'article 10 de la Convention européenne des droits de l'homme, devrait contenir certaines garanties pour éviter les risques d'abus et d'arbitraire[714]. Pour ces raisons, il serait, selon nous, judicieux et conforme à la *ratio legis* de l'article 39*bis* C.I.Cr. de laisser cette compétence au juge d'instruction. Compétence qu'il pourrait exercer sur la base de l'article 88*quater* C.I.Cr., mesure qui prévoit une obligation de collaboration à l'égard des personnes présumées disposer d'une connaissance particulière du système en cause.

224. Le blocage de site internet, une procédure qui doit être encadrée par le droit interne. Dans un arrêt du 18 décembre 2012[715], la Cour européenne des droits de l'homme se prononce sur une mesure de blocage de site internet prise par un tribunal. Ce dernier avait ordonné de bloquer l'accès à « Google sites » afin d'empêcher l'accès à un site internet dont le propriétaire était poursuivi pour outrage à la mémoire d'Atatürk. Le requérant, personne tiers à la procédure, invoquait la violation du droit à la liberté d'expression, celui-ci ne pouvant plus accéder à son propre site internet alors qu'il n'était pas lié aux poursuites pénales entamées. La Cour constate la violation de l'article 10 de la CEDH en raison de l'absence de détermination suffisante du cadre légal. De plus, selon la Cour, la procédure ne permet pas d'offrir des garanties suffisantes contre les risques d'abus et d'arbitraire. Cet arrêt met en lumière l'importance de prévoir un cadre légal strict *a contrario* de ce qu'il ressort de l'arrêt de la Cour de cassation du 22 octobre 2013[716] exposé *supra*.

2. Interception des télécommunications

225. Interception d'une communication par une personne y prenant part. Le secret des télécommunications est une facette du droit à la vie privée protégé par l'article 8 de la Convention européenne des droits de l'homme et l'article 22 de la Constitution. En principe, il est interdit de prendre connaissance du contenu des télécommunications sans en avoir l'autorisation. Néanmoins, les articles 90*ter* et suivants C.I.Cr. autorisent le juge d'instruction d'intercepter les télécommunications en « cours de transmission » en cas d'investigations liées aux infractions et tentatives d'infractions les plus graves[717]. Dans un arrêt du 8 janvier 2014[718], la Cour de cassation dit pour droit qu'une personne peut prendre connaissance et enregistrer le contenu d'une télécommunication sans l'accord de son interlocuteur pour autant qu'elle y participe elle-même. Cet enregistrement n'est pas une mesure d'interception des télécommunications au sens des articles 90*ter* et suivants C.I.Cr. même si la personne souhaite utiliser les éléments recueillis à titre de preuve[719].

---

713 R. Schoefs, « Changement de méthode dans la lutte contre The Pirate Bay : la saisie de données autorisée », note sous Cass., 22 octobre 2013, R.G. n^{os} P.13.0550.N et P.13.0551.N, *T. Strafr.*, 2014/2, pp. 131-142.

714 Q. Van Enis, « Les mesures de filtrage et de blocage de contenus sur l'internet : un mal (vraiment) nécessaire dans une société démocratique ? Quelques réflexions autour de la liberté d'expression », *Rev. trim. dr. h.*, n° 96, pp. 879 et s.

715 Cour eur. D.H., 18 décembre 2012, arrêt *Hüseyİn Yildirim c. Turquie*, n° 2778/02.

716 Cass. (2^{e} ch., sect. nl.), 22 octobre 2013, R.G. n° P.13.0550.N, www.cass.be.

717 Art. 90*ter*, §§ 2 et 3, C.I.Cr.

718 Cass. (2^{e} ch.), 8 janvier 2014, R.G. n° P.13.1935.F, www.cass.be.

719 K. Rosier, « Enregistrement d'une télécommunication à des fins de dénonciation », *B.S.J.*, n° 514, 2014, p. 16.

226. Pas d'ordonnance distincte pour le repérage et l'interception des télécommunications. Le juge d'instruction peut prescrire dans une seule ordonnance le repérage et l'écoute de communications privées au sens des articles 88*bis* et 90*quater* C.I.Cr. Si le dispositif de l'ordonnance ne prévoit que le repérage de communications électroniques, la mesure d'écoute peut valablement être ordonnée pour autant que l'ordonnance soit correctement motivée[720].

3. Observations

227. Principe. L'article 47*sexies* du Code d'instruction criminelle régit « l'observation systématique, par un fonctionnaire de police, d'une ou de plusieurs personnes, de leur présence ou de leur comportement, ou de choses, de lieux ou d'événements déterminés ». Est notamment considérée comme systématique, l'observation « dans le cadre de laquelle des moyens techniques sont utilisés »[721]. Une telle mesure est strictement encadrée, ne peut être mise en œuvre que par les services de police après autorisation par le procureur du Roi, dans le cadre de l'information, si les nécessités de l'enquête l'exigent et si les autres moyens d'investigation ne semblent pas suffire à la manifestation de la vérité. De surcroît, une observation effectuée à l'aide de moyens techniques ne peut être autorisée que lorsqu'il existe des indices sérieux que les infractions sont de nature à entraîner un emprisonnement correctionnel principal d'un an ou une peine plus lourde. Enfin, lorsque l'observation systématique est utilisée pour entamer une enquête proactive[722], on notera qu'est requise l'autorisation écrite et préalable du procureur du Roi.

228. Observation via un tiers exclue de l'article 47*sexies* C.I.Cr. Dans son arrêt du 19 juin 2012, la Cour de cassation jugea que l'utilisation, par des enquêteurs, de l'information obtenue par un moyen technique dont dispose un tiers qui met à la disposition des services de recherche les données qu'il a recueillies, ne constitue pas une observation au cours de laquelle un fonctionnaire de police utilise des moyens techniques requérant une autorisation[723]. En l'espèce, des enquêteurs de l'administration des douanes et accises avaient eu accès aux données d'un système automatisé « *tracking and tracing* » mis volontairement à leur disposition par une entreprise portuaire. La Cour ne contesta pas que ce système de localisation – permettant aux entreprises privées de suivre les conteneurs tant sur mer que sur terre, via une connexion internet sécurisée – constitue un moyen technique au sens de l'article 47*sexies*, § 1er, alinéa 3, du Code d'instruction criminelle. Grâce à ce système de localisation mis à leur disposition, les enquêteurs purent constater que les conteneurs litigieux avaient été déchargés du navire à Zeebrugge et ensuite transportés par train vers Anvers, où les marchandises ont été débarquées au port. Le trajet des conteneurs de Zeebrugge à Anvers dura plus ou moins quatre jours durant lesquels

720 Cass. (2e ch.), 24 septembre 2014, R.G. n° P.14.0915.F, www.cass.be.

721 Selon l'article 47*sexies* du Code d'instruction criminelle, est un moyen technique « une configuration de composants qui détecte des signaux, les transmet, active leur enregistrement et enregistre les signaux, à l'exception des moyens techniques utilisés en vue de l'exécution d'une mesure visée à l'article 90*ter* ».

722 Selon l'article 28*bis* du Code d'instruction criminelle : « Celle-ci, dans le but de permettre la poursuite d'auteurs d'infractions, consiste en la recherche, la collecte, l'enregistrement et le traitement de données et d'informations sur la base d'une suspicion raisonnable que des faits punissables vont être commis ou ont été commis mais ne sont pas encore connus, et qui sont ou seraient commis dans le cadre d'une organisation criminelle, telle que définie par la loi, ou constituent ou constitueraient un crime ou un délit tel que visé à l'article 90*ter*, §§ 2, 3 et 4 ».

723 Cass. (2e ch., sect. nl.), 19 juin 2012, R.G. n° P.12.0362.N, *Larcier cass.*, 2012/10, p. 231.

les enquêteurs purent suivre leur localisation grâce au système susmentionné[724]. La Cour considéra que « nonobstant le fait que les entreprises privées sécurisent l'obtention de ces données vis-à-vis du monde extérieur, rien ne les empêchait de partager ces données avec des tiers, dont les services de police ». Par cette simple assertion, la Cour de cassation jugea légalement justifiée la décision de la cour d'appel suivant laquelle la localisation des conteneurs sur la base de ces données, ne constitue pas une observation systématique requérant une autorisation. Nous ne pouvons nous rallier à un tel raisonnement. Il nous paraît essentiel que le critère emportant l'application des garanties procédurales prévues par l'article 47*sexies* C.I.Cr. reste l'objectif, par les forces de l'ordre, « d'observer de manière systématique » ; que cet objectif soit réalisé grâce à leurs propres moyens ou par le biais de moyens mis à leur disposition par des tiers. Dans un arrêt du 13 mai 2011[725], la cour d'appel de Bruxelles se prononça de manière conforme à ce principe, rappelant qu'un détournement de finalité d'un système d'information par les forces de police dans un but d'observation de personnes déterminées fait rentrer cette méthode d'enquête dans le champ d'application de l'article 47*sexies* C.I.Cr.

V. COMMUNICATIONS ÉLECTRONIQUES

Elise Defreyne[726], Christian Hocepied[727], Julien Jost[728],
Robert Queck[729], avec la collaboration de Rosario Debilio[730] [731]

A. Champ de la chronique

229. Le cadre réglementaire européen des réseaux et services de communications électroniques. Au niveau européen, le cadre réglementaire sectoriel pour les réseaux et services de communications électroniques actuellement en vigueur a été adopté en 2002 pour entrer en

724 Y. Van Den Berge : « Le système informatique automatisé "tracking et tracing" aux fins de localisation de conteneurs n'est pas une observation au sens de l'article 47*sexies* C.I.cr. », note sous Cass., 19 juin 2012, R.G. n° P.12.0363.N, *T. Strafr.*, 2013/3, p. 185.

725 Bruxelles (12e ch.), 13 mai 2011, *T. Strafr.*, 2012/5, p. 351. Dans le cas d'espèce, après avoir constaté de visu, sur le terrain, le manège suspect de trafic de drogue du prévenu, des policiers tentèrent en vain de l'appréhender. Ils découvrirent, cachés sous le pneu d'un véhicule, vers lequel ce prévenu s'était baissé à plusieurs reprises, dix pacsons de marihuana. C'est après cette première intervention, qui ne put être menée à bien, que les policiers décidèrent de se rendre au commissariat afin d'observer les allers et venues sur le lieu des faits grâce aux images enregistrées par cinq caméras placées sur la voie publique. Ces devoirs permirent de remarquer la présence du prévenu, ainsi que sa participation aux faits de la prévention. La cour d'appel estima que s'il va de soi qu'en cas de constat fortuit d'une infraction, au cours du visionnage d'images lors de ses missions, les policiers sont autorisés à intervenir et à conserver la preuve de l'infraction, tel n'est pas le cas lorsque le constat d'indices de (voire de simples informations relatives à) l'infraction a précédé le visionnage, comme en l'espèce. Pour cette raison, la cour jugea que les observations effectuées par les policiers relevaient bien du champ d'application de l'article 47*sexies* du Code d'instruction criminelle. Pour davantage de précisions, voy. F. Dumortier, « La surveillance par caméras : de la supervision de lieux vers l'observation systématique de personnes », in *Discipline et surveillance dans la relation de travail*, Limal, Anthemis, pp. 333-342.

726 Assistante à l'Université de Namur et chercheuse senior au CRIDS.

727 Chercheur senior au CRIDS.

728 Responsable de l'unité « Distributeurs et Opérateurs » du Conseil supérieur de l'audiovisuel (CSA).

729 Maître de conférences à l'Université de Namur et directeur-adjoint du CRIDS.

730 Conseiller juridique chez Darebe.

731 Les auteurs et collaborateurs s'expriment à titre personnel et n'engagent pas les institutions auxquelles ils appartiennent.