Criminalité informatique

Omrani, Feyrouze; Dumortier, Franck

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

Publication date:
2012

Document Version
le PDF de l'éditeur

atteinte par son comportement à une concurrence effective et non faussée dans le marché intérieur concerne précisément les comportements, actifs ou d'omission, que cette entreprise décide de sa propre initiative de mettre en œuvre »[1115].

VII. CRIMINALITÉ INFORMATIQUE[1116]

Feyrouze Omrani[1117] et Franck Dumortier[1118]

326*bis*. Introduction. Au cours des trois années de jurisprudence couverte par cette chronique 2009-2011, d'importantes décisions ont été prononcées en matière de hacking[1119], de possession d'images pédopornographiques[1120] (l'affaire *Hissel*) mais aussi quant à la notion de fournisseur de services de communications électroniques (l'affaire *Yahoo !*)[1121].

La présente chronique aborde successivement le faux en informatique, la fraude informatique, l'abus de confiance, le hacking, le délit de presse, le harcèlement et la possession d'image pédopornographique mais aussi des questions de procédures.

Bien qu'il soit prématuré de faire état d'une tendance à proprement parler, on relève que les cours et tribunaux ont appliqué des infractions de droit commun à des données informatiques dans le cadre du délit de presse et de l'abus de confiance.

A. Droit matériel

1. Faux en informatique

327. Faux en informatique dans un dossier infirmier. La Cour de cassation[1122] fut amenée à se prononcer sur un pourvoi dirigé contre un arrêt rendu par la cour d'appel de Gand dans un dossier d'abstention coupable d'un infirmier. Dans leur quatrième moyen, les demandeurs invoquent la violation du principe de non-rétroactivité au motif que l'arrêté royal déterminant les conditions générales minimales auxquelles doit répondre le dossier infirmier[1123] n'était pas encore entré en vigueur au moment des faits.

1115 C.J.U.E., 17 février 2011, *TeliaSonera Sverige AB*, C-52/09, *Rec.*, 2011, p. I-527, points 52-53.

1116 Bien que la présente chronique limite son examen aux décisions prononcées entre 2009 et 2011, nous tenons à évoquer deux éléments majeurs de l'année 2012, à savoir la ratification par la Belgique de la convention du Conseil de l'Europe sur la cybercriminalité le 20 août 2012 (convention adoptée à Budapest, le 23 novembre 2001 – STCE no. : 185. La loi de ratification est entrée en vigueur le 1er décembre 2012) et la création en juin 2012 du centre d'excellence B-CCENTRE (Belgian Cybercrime Centre of Excellence) (http://www.b-ccentre.be/). Ce centre a pour ambition, d'une part, de devenir une plate-forme de coordination pour la recherche sur la cybercriminalité et, d'autre part, d'assurer la formation et l'entraînement d'acteurs du secteur.

1117 Chercheuse au CRIDS, avocate au barreau de Bruxelles.

1118 Chercheur senior au CRIDS.

1119 Voy., *infra*, nos 333 et s.

1120 Voy., *infra*, nos 339 et s.

1121 Voy., *infra*, no 341.

1122 Cass. (2e ch.), 26 mai 2009, R.G. no P.09.0032.N.

1123 Arrêté royal du 28 décembre 2006 déterminant les conditions générales minimales auxquelles le dossier infirmier, visé à l'article 17, i), de la loi sur les hôpitaux, coordonnée le 7 août 1987, doit répondre, *M.B.*, 30 janvier 2007.

La Cour rejette l'argument et valide la motivation des juges du fond qui ne reposait pas sur l'irrespect de l'arrêté royal susmentionné mais sur la circonstance que constitue un faux en informatique le fait d'introduire consciemment des informations inexactes ou d'omettre des mentions essentielles et véridiques dans un dossier infirmier électronique avec pour conséquence que le traitement d'un patient n'ait pas pu être déterminé avec suffisamment de précision.

328. Tentative de faux en informatique lors d'un « test de sécurité » illégitime d'un site web. En juillet 2007, Fortis Banking constate que lors d'une connexion internet avec un client, un inconnu a essayé d'avoir accès à son système d'exploitation en utilisant un faux code pin dans le but d'exécuter un script lui permettant d'afficher une page web tierce au sein d'un *frame* du site de Fortis.

Rappelons que la qualification de faux en informatique requiert, d'une part, deux éléments matériels, d'autre part, un élément moral. Le premier élément matériel consiste à introduire, modifier ou effacer des données stockées, traitées ou transmises par un système informatique ou de modifier l'utilisation possible de celles-ci par tout moyen technologique. Le second – qui consiste à modifier la portée juridique de telles données – est une question de fait laissée à l'appréciation du juge. L'élément moral requis est, quant à lui, le dol spécial consistant en une intention frauduleuse ou un dessein de nuire[1124].

Dans son jugement du 15 juin 2010, le tribunal correctionnel de Louvain[1125] estime que la tentative de faux en informatique se matérialise dans le fait d'avoir tenté d'introduire des données informatiques incorrectes pour accéder à un système de PC Banking. S'agissant de la modification de la portée juridique des données, les juges la perçoivent dans deux circonstances : d'une part, dans le fait d'avoir utilisé un code pin ne permettant pas à la banque d'identifier automatiquement son ayant droit, d'autre part, dans le fait d'avoir utilisé un *script* après l'introduction de ce faux code dans l'intention de tromper la banque mais aussi des tiers.

En ce qui concerne l'élément moral, l'argument du prévenu selon lequel il avait simplement l'intention de tester la sécurité du système afin que la banque puisse mieux le protéger n'est pas suivi par les juges au motif que lorsque l'on procède à un tel test, on examine si et comment le système réagit à l'apport d'un facteur numérique inconnu et quelles en sont les incidences positives ou négatives possibles (lire « les conséquences dommageables »). L'intention frauduleuse est, en d'autres termes, inhérente au test effectué sur un système informatique[1126]. Il n'est pas requis à cet égard que le préjudice soit effectivement réalisé, un préjudice potentiel suffit.

329. Autres applications de faux en informatique. Le tribunal correctionnel de Termonde a jugé que le fait, pour une société, de se faire passer pour l'Institut national des statistiques en utilisant l'adresse URL www.nis-be.com et des adresses e-mail correspondantes dans le but d'ob-

[1124] Voy. l'article 193 du Code pénal selon lequel « le faux commis en écritures, *en informatique,* ou dans les dépêches télégraphiques, avec une intention frauduleuse ou à dessein de nuire, sera puni conformément aux articles suivants » (nous soulignons).

[1125] Corr. Louvain, 15 juin 2010, *T. Strafr.,* 2011/04, p. 270.

[1126] De la même manière, il a été jugé que l'utilisation d'une méthode d'attaque peu et mal élaborée lors d'une tentative de hacking ne signifiait pas qu'il n'y avait pas d'intention frauduleuse ou de dessein de nuire. Voy. Corr. Termonde, 2 février 2009, inédit, cité par J. Kerkhofs et P. Van Linthout, « Cybercriminaliteit doorgelicht », *T. Strafr.*, 2010/4, p. 182.

tenir plus rapidement les chiffres d'affaires et d'autres informations de la part de PMEs, modifie la portée juridique de ces données[1127].

Il en a été jugé de même pour la création et l'utilisation d'un profil *Netlog* au nom d'une autre personne[1128].

2. Fraude informatique

330. Principe. Constitue une fraude informatique au sens de l'article 504*quater* du Code pénal, le fait, pour un fonctionnaire du SPF Finances, d'utiliser son accès au système informatique de l'administration afin d'augmenter le montant du précompte professionnel dans son propre dossier afin d'être remboursé annuellement par le fisc de plusieurs milliers d'euros supplémentaires[1129].

331. Cause absolutoire. Il est également intéressant de relever que le tribunal de première instance de Hasselt, chambre correctionnelle, a rappelé que la cause absolutoire relative à la parenté prévue à l'article 462 du Code pénal s'applique également au délit de fraude informatique[1130].

3. Abus de confiance appliqué aux données informatiques

332. Objets qui peuvent faire l'objet d'un abus de confiance. L'article 491 du Code pénal énumère les objets qui peuvent faire l'objet d'un abus de confiance, à savoir « les effet, deniers, marchandises, billets, quittances, écrits de toute nature contenant ou opérant obligation de décharge ». Cette liste est limitative et vise tout objet mobilier corporel ayant une valeur financière[1131]. Les écrits visés par cette disposition sont ceux qui contiennent ou opèrent obligation de décharge mais il avait déjà été jugé qu'un écrit qui ne contient ou n'opère ni obligation ni décharge pourrait toutefois être l'objet d'un abus de confiance lorsqu'il constitue une marchandise[1132] ou représente une valeur marchande[1133].

Dans un arrêt du 5 janvier 2011[1134] relatif à des employés poursuivis pour avoir fait un *back-up* de données informatiques d'un site et de courriers électroniques des administrateurs et des employés d'une société et pour avoir manipulé et conservé ces données par-devers eux à leur propre usage, la Cour de cassation estime que des logiciels, études, rapports, documents contractuels, listes de contacts et autres outils de gestion, figurant dans un système informatique peuvent être assimilés aux écrits de toute nature ou autres objets mobiliers corporels lorsque ces écrits constituent une marchandise ou ont une valeur économique. En l'espèce, la Cour considère qu'en

1127 Corr. Termonde, 13 février 2009, inédit, cité par J. Kerkhofs et P. Van Linthout, *op. cit.*, p. 182.

1128 Corr. Termonde, 21 décembre 2009, inédit, cité par J. Kerkhofs et P. Van Linthout, *op. cit.*, p. 182.

1129 Corr. Termonde, 15 janvier 2010, inédit, cité par J. Kerkhofs et P. Van Linthout, *op. cit.*, p. 184.

1130 Corr. Hasselt, 24 février 2010, N. C., 2010, p. 256.

1131 H.-D. Bosly, « L'abus de confiance », in H.-D. Bosly et C. De Valkeneer, *Les infractions contre les biens*, Bruxelles, Larcier, 2008, pp. 416-417.

1132 En son temps, confrontée à l'évolution technologique, la Cour de cassation avait été appelée à trancher une question similaire à propos du courant électrique : elle a considéré que le juge du fond pouvait légalement décider que le courant électrique était une marchandise au sens de l'article 491 du Code pénal. Voy. Cass., 20 juin 1934, *Pas.*, 1934, p. 332.

1133 Cass., 29 novembre 2000, R.G. n° P.00.1098.F, *Pas.*, 2000, n° 655 ; A. De Nauw, *Initiation au droit pénal spécial*, Waterloo, Kluwer, 2008, p. 457.

1134 Cass. (2e ch.), 5 janvier 2011, R.G. n° P.10.1094.F.

constatant que les données en question étaient dépourvues de toute valeur marchande, les juges du fond pouvaient légalement décider que ces données n'étaient pas des choses susceptibles d'être détournées.

4. Hacking

333. Hacking interne ou externe. Le paragraphe 1er de l'article 550*bis* du Code pénal réprime l'accès non autorisé à un système informatique ou le fait de s'y maintenir (hacking externe), tandis que son paragraphe 2 vise celui qui, avec une intention frauduleuse ou dans le but de nuire, outrepasse son pouvoir d'accès à un système informatique (hacking interne). On remarquera que l'élément moral requis diffère dans les deux hypothèses. Un dol spécial est exigé dans le seul cas du hacking interne. En revanche, un dol général suffit pour la prévention de hacking externe[1135]. À noter que si l'infraction est commise avec une intention frauduleuse, la peine s'en trouve seulement aggravée[1136].

Le tribunal correctionnel de Louvain[1137] fut amené à examiner la distinction entre ces deux formes de hacking suite à une tentative d'accès par un client de Fortis au système d'exploitation de la banque en utilisant un faux code pin dans le but d'exécuter un *script* lui permettant d'afficher une page web tierce au sein d'une *frame* du site de Fortis et de tromper des tiers. Selon le tribunal, le fait d'être client de Fortis et de disposer d'un Digipass lui permettant d'utiliser les services de PC Banking ne donne pas au prévenu la qualité d'utilisateur interne à Fortis. Les juges estiment en effet qu'il n'est pas dans l'intention du législateur de conférer à quasi chaque citoyen adulte la qualité d'utilisateur interne du système bancaire.

334. Dépassement d'accès à un système informatique. Dans l'arrêt du 5 janvier 2011[1138] précité, la Cour de cassation se penche sur un pourvoi dirigé contre une décision[1139] dans laquelle les premiers défendeurs sont prévenus du fait d'avoir, avec une intention frauduleuse ou à dessein de nuire, outrepassé leur pouvoir d'accès à un système informatique, avec la circonstance qu'ils en ont repris les données, en ont fait usage ou lui ont causé un dommage quelconque (hacking interne). Les premiers défendeurs avaient fait un *back-up* sur cd-rom de données informatiques du site FTP et de courriers électroniques des administrateurs et employés d'une société à la demande du premier défendeur qui avait le droit d'accéder à ces données lorsqu'il a demandé et obtenu le cd-rom. La Cour de cassation confirme le raisonnement de la cour d'appel et rejette le moyen en estimant que la constatation selon laquelle les premiers défendeurs avaient le droit d'accéder aux données litigieuses lorsque le premier en a demandé et obtenu la copie exclut le dépassement de pouvoir d'accès incriminé à l'article 550*bis*, § 2, du Code pénal. La Cour de cassation estime en outre que la cour d'appel n'avait pas à vérifier si les premiers défendeurs se sont maintenus dans le système informatique ou y ont accédé après leur démission (hacking externe) puisqu'ils n'étaient pas poursuivis sur la base de l'article 550*bis*, § 1er, du même code.

1135 Notons à ce sujet qu'il a récemment été jugé que n'est pas exempté de dol général un sujet néerlandais qui se prévaut de son ignorance de la sévérité de la loi belge. Voy. Corr. Termonde, 5 octobre 2009, inédit, cité par J. Kerkhofs et P. Van Linthout, *op. cit.*, p. 186.

1136 O. Leroux, « Criminalité informatique », *Les infractions contre les biens*, Bruxelles, Larcier, 2008, p. 398.

1137 Corr. Louvain, 15 juin 2010, *T. Strafr.*, 2011/04, p. 270.

1138 Cass. (2e ch.), 5 janvier 2011, R.G. no P.10.1094.F.

1139 Liège, 20 mai 2010, *T. Strafr.*, 2012, p. 175, note J. Coppens.

335. Tentative de hacking. L'article 550*bis*, § 4, du Code pénal punit la tentative de hacking des mêmes peines que le délit consommé. Selon certains auteurs, l'intention du législateur est d'incriminer la mise en danger que de tels actes peuvent entraîner[1140]. Dans les faits ayant donné lieu à une décision du tribunal de première instance de Termonde – chambre correctionnelle – du 2 février 2009[1141], un homme avait tenté d'accéder aux comptes e-mail de son précédent employeur en essayant un grand nombre de mots de passe et en appuyant 6112 fois sur le bouton « mot de passe oublié ». Les faits ont également été qualifiés de sabotage informatique, délit prévu par l'article 550*ter*[1142], étant donné qu'en conséquence des actes du prévenu, 6112 mails ont été envoyés sur la messagerie dudit employeur entraînant une surcharge du système informatique *(mailbombing)*. En outre, les juges ont considéré que les faits entrainaient la violation de l'article 145, § 3*bis*, de la loi du 13 juin 2005 relative aux communications électroniques qui punit 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 ».

336. *Hackertools*. L'article 550*bis*, § 5, du Code pénal punit celui qui, indûment, possède, produit, vend, obtient en vue de son utilisation, importe, diffuse ou met à disposition sous une autre forme, un quelconque dispositif, y compris des données informatiques, principalement conçu ou adapté pour permettre le hacking. Le tribunal de première instance de Termonde – chambre correctionnelle –[1143] a considéré que cette disposition s'appliquait à celui qui télécharge sur Internet un programme permettant d'activer la webcam de tiers à distance[1144].

5. Délit de presse sur internet

336*bis*. Délit de presse sur un site web. Dans une affaire traitée par le tribunal de première instance de Bruxelles – chambre correctionnelle –[1145], les prévenus ont été renvoyés devant le tribunal notamment pour avoir diffusé sur internet des textes visés par la loi Moureaux[1146], incitant à la discrimination, à la ségrégation, à la haine ou à la violence à l'égard d'un groupe, d'une communauté ou de leurs membres, en raison de la race, de la couleur, de l'ascendance ou de l'origine nationale ou ethnique de ceux-ci ou de certains d'entre eux.

L'intérêt de cette décision repose sur la réponse apportée à la question de savoir si un délit de presse peut se réaliser sur le net sans qu'il y ait de recours à un procédé technique de reproduction. Le tribunal répond par l'affirmative en ces termes « le délit de presse doit également s'appliquer lorsque la diffusion est effectuée par la voie de l'Internet ». L'absence de justification s'explique peut-être par le fait qu'un des prévenus faisait valoir précisément cette interprétation comme moyen de défense.

1140 *Ibidem*.
1141 Corr. Termonde, 2 février 2009, inédit, cité par J. Kerkhofs et P. Van Linthout, *op. cit.*, p. 187.
1142 Le sabotage informatique vise des actes de destruction tels que la destruction de fichiers ou le fait de rendre inutilisable un système, ou encore la conception et/ou la diffusion de virus.
1143 Corr. Termonde, 1er mars 2010, inédit, cité par J. Kerkhofs et P. Van Linthout, *op. cit.*, p. 188.
1144 Voy. Corr. Termonde, 1er mars 2010, inédit, cité par J. Kerkhofs et P. Van Linthout, *op. cit.*, p. 188.
1145 Corr. Bruxelles, 23 juin 2009, inédit.
1146 Loi du 30 juillet 1981 tendant à réprimer certains actes inspirés par le racisme ou la xénophobie.

336*ter*. Délit de presse et commentaires de vidéos postées sur internet. Le discours, tenu par un homme politique à la suite d'une manifestation organisée par un groupe citoyen œuvrant pour le respect des droits et la protection du peuple palestinien, est mis en ligne par le comité de coordination des organisations juives de Belgique et le directeur de celui-ci sur le propre site internet du comité mais aussi sur Youtube. Sur les deux sites, la vidéo est accompagnée d'un commentaire accusant l'homme politique d'antisémitisme. Le tribunal de première instance de Bruxelles considère dans son jugement du 15 octobre 2009[1147] que « la notion de presse doit être entendue au sens large en tenant compte de l'évolution des techniques et constate à cet égard que les sites internet sont des moyens habituels de transmission d'informations et d'opinions ». Il retient la qualification de délit de presse bien qu'en l'espèce « le média utilisé n'est pas à proprement parler un imprimé ».

336*quater*. Délit de presse sur un blog. La cour d'appel de Bruxelles est appelée à connaître de l'affaire suivante : le prévenu est poursuivi pour avoir tenu des propos diffamatoires à l'encontre d'un officier de police dans le cadre d'un forum de discussion d'un site web. En l'espèce, le policier est accusé par le prévenu de rédiger des procès-verbaux tendancieux et de manipuler les magistrats.

La première question que doit trancher la cour d'appel est relative à sa compétence puisque l'article 150 de la Constitution réserve à la Cour d'assise la compétence exclusive de connaître du délit de presse. Le 17 mars 2010[1148], la Cour conclut à son incompétence *ratione materiae* dès lors que « À s'en tenir à la question du support technique utilisé pour la diffusion d'écrits, on ne concevrait pas qu'un même article ou commentaire litigieux publié dans un journal quotidien puisse relever du délit de presse dans sa version ''papier'' et y échapper dans sa version identique mais diffusée sur Internet ».

On peut d'ores et déjà indiquer que la Cour de cassation suivra la jurisprudence précitée puisqu'à l'occasion de deux arrêts du 6 mars 2012[1149], elle a résolument fait le choix d'une interprétation évolutive et téléologique du délit de presse en admettant qu'il s'applique aux écrits diffusés sur internet.

6. Harcèlement et technologies de la communication

337. Harcèlement et courriers électroniques émis par un parti politique par courriers électroniques. Après avoir admis que le fait de recevoir des courriers électroniques émanant d'une formation politique dont on réprouve radicalement les opinions constitue un réel désagré-

1147 Civ. Bruxelles (75e ch.), 15 octobre 2009, *J.T.*, n° 6391, 15/2010, pp. 254-258, *J.L.M.B.*, 3/2010, pp. 128-137, et sa note C. Dony, « La presse, une notion que le Constituant tarde à (re)définir… », *ibidem*, pp. 37-142.

1148 Bruxelles (11e ch. civ.), 17 mars 2010, *J.T.*, n° 6405, 29/2010, p. 506 et sa note Q. Van Enis, « Le ''délit de presse'' sur l'internet : seul le jury populaire est compétent pour sanctionner pénalement le ''chien de garde'' qui aurait crié au loup… », *ibidem*, pp. 506-509.

1149 Cass. (2e ch.), 6 mars 2012, n° P.11.0855.N/1, *NjW*, 2012, liv. 262, p. 342 et Cass., 6 mars 2012, n° P.11.1374.N, *NjW*, 2012, liv. 262, p. 341. Voy. *supra* n° 176 et aussi la note d'observations de 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.*, n° 6483, 23/2012, pp. 505-507.

ment, la cour d'appel de Bruxelles, par un arrêt du 17 mars 2010[1150], conclut qu'en l'espèce cela ne suffit pas à admettre qu'un tel comportement serait de nature à compromettre la tranquillité de la personne concernée au sens de l'article 442*bis* du Code pénal. Il est requis que l'auteur supposé du harcèlement ait su ou ait dû savoir qu'il affecterait gravement la tranquillité de la plaignante. En l'espèce, il n'est pas établi que le prévenu avait conscience d'importuner la plaignante[1151].

338. Harcèlement et communications électroniques. Saisie sur question préjudicielle, la Cour constitutionnelle, dans son arrêt du 22 décembre 2011[1152], a examiné si l'article 145, § 3*bis,* de la loi du 13 juin 2005 relative aux communications électroniques violait les articles 10 et 11 de la Constitution, d'une part, parce qu'il ne prévoit pas comme condition de recevabilité des poursuites une demande expresse de la victime contrairement à l'article 442*bis* du Code pénal, d'autre part, parce qu'il incrimine le fait d'importuner un correspondant alors qu'aucune prévention n'existe quand on importune un tiers avec un autre moyen de communication. La Cour suprême a reconnu le traitement différentiel mais n'a pas conclu à une violation des principes d'égalité et de non-discrimination. Il résulte des travaux préparatoires qu'il s'agit d'une décision délibérée du législateur de traiter différemment le harcèlement réalisé au moyen d'un réseau de communications électroniques. Selon la Cour, ceci résulte de ce que « l'usage des communications électroniques a en effet pu être considéré comme constituant une source d'abus plus importants que dans d'autres domaines ».

Dans le cadre de l'article 145, § 3*bis* de la loi du 13 juin 2005, il « n'est ni requis que l'utilisation du moyen de télécommunication présente un caractère harcelant ni que la tranquillité du correspondant de la personne soit effectivement perturbée ». L'élément déterminant est l'élément moral dans le chef du contrevenant, à savoir la volonté d'importuner son correspondant.

*7. La possession d'images pédopornographiques – L'article 383***bis***, § 2, du Code pénal*

339. Introduction. La loi du 13 avril 1995 relative aux abus sexuels à l'égard des mineurs a introduit l'article 383*bis*, § 2 ancien du Code pénal qui punit d'un emprisonnement d'un mois à un an et d'une amende de cent euros à mille euros quiconque aura sciemment *possédé* les emblèmes, objets, films, photos, diapositives ou autres supports visuels qui représentent des positions ou des actes sexuels à caractère pornographique, impliquant ou présentant des mineurs.

340. Vision d'images pédopornographiques. À l'occasion de deux affaires, la Cour de cassation est amenée à se pencher sur la notion de possession d'images pédopornographiques.

Dans la première affaire du 20 avril 2011[1153], le demandeur avait accédé à un site informatique au départ duquel il visionnait des images de pornographie enfantine. Il n'avait ni imprimé ces images ni conservé de copie de celles-ci sur son ordinateur. Pour cette raison, le demandeur fait grief à la cour d'appel de Liège d'avoir violé l'article 383*bis*, § 2, du Code pénal en lui donnant

1150 Bruxelles (11e ch. corr.), 17 mars 2010, *R.D.T.I.*, n° 42/2011, pp. 51-54 et la note d'observations de F. Coppens, « Quatre questions sur le spamming politique ».

1151 Sur la question de l'assimilation de ces courriels électroniques au spamming politique, voy. *supra*, n° 4.

1152 Cour const., arrêt n° 198/2011 du 22 décembre 2011.

1153 Cass. (2e ch.), 20 avril 2011, *R.D.T.I.*, n° 44/2011, pp. 27-28 suivi de la note d'observations de N. Blaise, « L'interdiction de consulter des images pédopornographiques sur internet : avancée ou précision ? ».

une interprétation par analogie. Il conteste, en effet, que la consultation d'image pédopornographique soit incriminée par cette disposition qui vise la seule possession de telles images.

Après avoir rappelé que la *ratio legis* de la loi du 13 avril 1995 précitée est de sanctionner le simple consommateur de matériel pédopornographique, la Cour de cassation précise que « la possession (au sens de l'article 383*bis* du Code pénal) ne requiert pas que l'utilisateur d'un ordinateur manifeste sa maîtrise de l'image par le téléchargement ou l'impression de celle-ci ni qu'il la détienne de manière continue ». Forte de son interprétation téléologique, la Cour de cassation affirme que « le seul fait d'accéder à un site informatique et de visionner les images, *en connaissance de cause*, suffit, cette consultation impliquant que le demandeur a été en possession d'un écran d'ordinateur montrant de la pornographie enfantine »[1154].

Dans une seconde affaire du 26 octobre 2011[1155], la Cour de cassation connaît de la même problématique que celle dont elle était saisie à l'occasion de l'arrêt du 20 avril 2011. Elle confirme la position qu'elle avait retenue alors mais enrichit sa réflexion du raisonnement du juge d'appel qu'elle reprend à son compte. Elle retient, en effet, que « dans son sens usuel, la possession se définit comme la faculté actuelle de disposer ou de jouir d'un bien ». Aussi, « en ouvrant les images, le demandeur en a disposé dès lors qu'il lui était loisible, pendant le temps du visionnage, de leur réserver l'emploi qu'il souhaitait et qu'il dépendait de sa seule volonté de déterminer le temps du visionnage, de les télécharger ou de les imprimer ».

La position de la Cour de cassation a posé question au regard du principe d'interprétation stricte du droit pénal illustré par les adages *nulla crimen sine lege* et *nulla pene sine lege*[1156]. Pour N. Blaise, en faveur de l'interprétation téléologique à laquelle la Cour de cassation s'est prêtée, le champ d'application de l'article 383*bis* du Code pénal ne s'est pas étendu mais uniquement vu confirmé.

Il est à noter qu'à l'occasion de la proposition de loi modifiant la législation en ce qui concerne l'amélioration de l'approche des abus sexuels et des faits de pédophilie dans une relation d'autorité[1157] et déposée le 29 juin 2011, soit postérieurement à cet arrêt, le législateur a ressenti la nécessité d'étendre[1158] le champ d'incrimination de la pédopornographie. Il est vrai que cette nécessité résulte notamment de la volonté de transposer en droit belge certaines dispositions issues de la Convention de Lanzarote[1159]. Les travaux préparatoires de la proposition énoncent cependant que « le fait d'accéder, en connaissance de cause et par le biais des technologies de communication et d'information, à de la pornographie enfantine doit également être sanctionné, n'a en revanche

1154 Nous soulignons.

1155 Cass. (2e ch.), 26 octobre 2011, *J.L.M.B.*, 2012/10, pp. 449-451 suivi de la note d'observations de N. Colette-Basecqz, « La notion de possession de supports pédopornographiques : les délicates questions soulevées par l'interprétation de la loi pénale ». Cette affaire fait actuellement l'objet d'un pourvoi devant la Cour européenne des droits de l'homme.

1156 N. Colette-Basecqz, « La notion de possession de supports pédopornographiques : les délicates questions soulevées par l'interprétation de la loi pénale », note sous Cass. (2e ch.), 26 octobre 2011, *J.L.M.B.*, 2012/10, p. 455.

1157 *Doc. parl.*, Ch. repr., sess. ord. 2010-2011, lég. 53, n° 1639/001, pp. 8-11.

1158 Le choix du verbe « étendre » n'est pas anodin puisque le titre du chapitre 5 consacré à cette question est intitulé « De l'extension de l'incrimination de la pédopornographie ». Voy. en ce sens *Doc. parl.*, Ch. repr., sess. ord. 2010-2011, lég. 53, n° 1639/001, p. 8. Notons qu'ultérieurement le chapitre changera d'intitulé « De la clarification de l'incrimination de la pédopornographie ». Voy. en ce sens *Doc. parl.*, Ch. repr., sess. ord. 2010-2011, lég. 53, n° 1639/003, p. 26.

1159 Convention du 25 octobre 2007 du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels qui, au moment de la modification de la loi, a été signée par la Belgique (dès le 25 octobre 2007) mais non encore ratifiée à ce jour.

pas encore été inséré dans le Code pénal belge »[1160]. Pour certains parlementaires, la mise en conformité du droit belge à la Convention de Lanzarote permettrait en réalité de « mettre fin à un problème d'interprétation de la législation existante »[1161]. Pour d'autres, « le fait qu'un parlementaire estime devoir proposer une modification de la loi existante, sans qu'il apparaisse qu'il soit nécessairement correctement informé de la portée de celle-ci, n'est démonstratif ni du bien fondé, et dès lors, du succès de sa démarche, ni singulièrement en conséquence de l'existence réelle d'une lacune législative à combler »[1162].

340*bis*. Modification législative. La polémique a pris fin avec l'adoption, le 30 novembre 2011, de la loi modifiant la législation en ce qui concerne l'amélioration de l'approche des abus sexuels et des faits de pédophilie dans une relation d'autorité. Désormais, l'article 383*bis* nouveau du Code pénal se lit comme suit : « quiconque aura sciemment possédé les emblèmes, objets, films, photos, diapositives ou autres supports visuels visés sous le § 1er *ou y aura, en connaissance de cause, accédé par un système informatique ou par tout moyen technologique*, sera puni d'un emprisonnement d'un mois à un an et d'une amende de cent euros à mille euros »[1163].

B. Questions de procédure

341. Obligation de collaboration. Au départ de l'affaire *Yahoo !*[1164] traitée par la Cour de cassation dans son arrêt du 8 janvier 2011, plusieurs personnes ont commandé par internet des ordinateurs payés au moyen de cartes bancaires détournées par *phishing*[1165]. Pour perpétrer leurs méfaits, ceux-ci ont utilisé un compte e-mail Yahoo !. Afin de poursuivre ces individus, le procureur du Roi a essayé d'obtenir, de la part de Yahoo !, des données d'identification les concernant sur la base de l'article 46*bis* du Code d'instruction criminelle selon lequel il peut requérir le concours de l'opérateur d'un réseau de communication électronique ou d'un fournisseur d'un service de communication électronique pour identifier l'abonné ou l'utilisateur habituel d'un service. Yahoo ! a refusé de faire droit à la demande du Parquet en avançant qu'il n'était pas un « fournisseur d'un service de communication électronique » au sens de l'article 46*bis* du Code d'instruction criminelle[1166].

1160 *Doc. parl.*, Ch. repr., sess. ord. 2010-2011, lég. 53, n° 1639/001, p. 10.

1161 *Doc. parl.*, Ch. repr., sess. ord. 2010-2011, lég. 53, n° 1639/003, p. 26.

1162 Liège, 23 mai 2011, inédit, cité par N. Blaise, « L'interdiction de consulter des images pédopornographiques sur internet : avancée ou précision ? », *R.D.T.I.*, n° 44/2011, p. 33.

1163 Nous soulignons.

1164 Cass., 8 janvier 2011, *R.D.T.I.*, 2011/44, p. 113. Pour un exposé exhaustif et une analyse de l'affaire *Yahoo !,* voy. 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.*, 44/2011, p. 116.

1165 Le *phishing* ou « hameçonnage » peut être défini comme une forme de criminalité informatique consistant dans le fait d'envoyer à des personnes un faux mail semblant provenir d'institutions financières ou de banques leur demandant de fournir ou de mettre à jour leurs données bancaires, données qui seront ensuite utilisées pour retirer de l'argent ou effectuer des paiements au préjudice des personnes visées. Voy. I. Delbrouck, « Criminalité informatique », in X., *Postal Memorialis. Lexique du droit pénal et des lois spéciales*, Waterloo, Kluwer, 2010, p. C362/16.

1166 En première instance, Yahoo ! a également usé d'un autre argument qui consistait à souligner l'incompétence des juridictions belges pour adresser une telle requête du fait que les données demandées étaient situées aux États-Unis. Pour une analyse de cet argument, nous renvoyons à la partie de cette chronique consacrée au droit international et européen, *infra*, n°s 343 et s.

En degré d'appel[1167], en se basant sur les travaux préparatoires de l'article 46*bis,* les juges avaient considéré que la notion de « fournisseur de services de communications électroniques » devait s'entendre au sens que lui donne la loi du 13 juin 2005 relative aux communications électroniques[1168]. Après avoir constaté que Yahoo ! mettait à la disposition de ses usagers des comptes de courrier électronique appartenant à son système webmail et que pour l'accès à ces comptes et la transmission des données qui y sont contenues, Yahoo ! faisait uniquement usage de l'infrastructure existante et n'intervenait pas personnellement dans le transfert des données, la cour d'appel de Gand a estimé qu'il ne pouvait pas être considéré comme un « fournisseur d'un service de communications » au sens de l'article 46*bis* du Code d'instruction criminelle.

La Cour de cassation ne fut pas du même avis et, en se référant au principe d'autonomie du droit pénal, décida que le fournisseur d'un service de télécommunications électroniques au sens de l'article 46*bis* du Code d'instruction criminelle « n'est pas uniquement l'opérateur belge au sens de la loi du 13 juin 2005 relative aux communications électroniques, mais quiconque dispense des services de communications électroniques, comme notamment la transmission de données de communication ». Selon la Cour, l'obligation de concours prévue par l'article 46*bis* du Code d'instruction criminelle ne se limite, dès lors, aux fournisseurs d'un service de communications électroniques qui sont aussi opérateurs au sens de la loi du 13 juin 2005 ou qui ne dispensent leurs services de communications électroniques qu'au moyen de leur propre infrastructure. Cette obligation existe aussi dans le chef de celui qui fournit un service consistant entièrement ou principalement dans la transmission de signaux par la voie des réseaux de communications électroniques et la personne qui fournit un service consistant à autoriser ses clients à obtenir ou recevoir ou diffuser des informations au moyen d'un réseau électronique peut aussi être un fournisseur d'un service de communications électroniques.

342. Proportionnalité des mesures d'identification. Le paragraphe 2 de l'article 46*bis* du Code d'instruction criminelle stipule que la motivation des mesures d'identification ordonnées par le procureur du Roi doit refléter le caractère proportionnel eu égard au respect de la vie privée et subsidiaire à tout autre devoir d'enquête. En l'espèce, un pourvoi en cassation est dirigé contre l'arrêt de la cour d'appel de Gand, chambre des mises en accusation, du 19 octobre 2010. Le demandeur fait valoir que la cour d'appel ne pouvait juger que la décision du procureur du Roi pour procéder à la mesure d'identification le concernant était légalement motivée puisque sa motivation ne consistait qu'en une formule de style ne contenant pas les éléments concrets la justifiant.

1167 Gand, 30 juin 2010, *T. Strafr.*, 2011, p. 132.

1168 Un « service de communication électronique » est défini par l'article 2, 5° de la loi du 13 juin 2005 relative aux communications électroniques comme étant 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 la 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 ».

La Cour de cassation[1169] rejette le pourvoi au motif que l'article 46*bis*, § 2, du Code d'instruction criminelle requiert uniquement que la décision du procureur du Roi soit motivée de telle sorte qu'il transparaisse à sa lecture qu'elle a été prise en tenant compte des exigences de proportionnalité et de subsidiarité. Selon la Cour, un tel type de motivation, ne contenant pas les éléments concrets la justifiant, n'empêche pas le juge du fond de se prononcer sur sa légalité.

VIII. DROIT INTERNATIONAL ET DROIT EUROPÉEN – L'INTENTION « GÉODÉTERMINÉE » : UN FACTEUR DE RATTACHEMENT CONFIRMÉ ?

Jean-Philippe Moiny[1170]

A. Introduction

343. Introduction. Une chronique de jurisprudence en matière de droit des TIC et de droit international privé se focalise rapidement sur l'Internet. Outre la structure classique du propos – compétence (B), droit applicable et libre prestation des services[1171] (C) –, requise à des fins de lisibilité, mais parfois impuissante à séparer efficacement et hermétiquement les développements[1172], une autre lecture de la jurisprudence étudiée, centrée sur Internet et plus transversale, est brièvement proposée à titre introductif.

Dans un sens, ce qui a lieu « sur Internet » n'est qu'un prolongement des activités du monde « physique », si l'on peut dire ; « *het internet is een plaats, weliswaar een virtuele plaats, maar een plaats waar dezelfede transacties kunnen gebeuren als in een reëel gebouw* […] »[1173]. Ce réseau présente néanmoins certaines spécificités parmi lesquelles nous retenons sa décentralisation et son accessibilité ubiquitaire. Sans aucun doute, celles-ci alimentent les discussions en droit international et le cas échéant, nécessitent des aménagements jurisprudentiels[1174].

344. Intention « géodéterminée ». Souvent, les juridictions rechignent, à juste titre, à assortir la simple accessibilité d'un site Web de conséquences juridiques, si bien qu'elles recherchent chez le prestataire de service, en appliquant les règles de droit international privé, une intention d'atteindre un marché national, de destiner son service à une audience particulière, de cibler des

1169 Cass., 29 mars 2011, R.G. n° P.10.1755.N., *T. Strafr.*, 2011/6, p. 426.

1170 Aspirant du F.R.S.-FNRS au CRIDS. L'auteur remercie vivement la professeure Stéphanie Francq pour sa relecture et ses commentaires avisés.

1171 S'il est vrai qu'à strictement parler, les décisions relatives à la libre prestation des services ne portent pas directement sur le droit international privé, elles ont néanmoins une incidence sur l'applicabilité des règles nationales aux situations comportant un élément d'extranéité, et méritent par conséquent d'être évoquées.

1172 La structure n'inclut en outre pas la question de la compétence territoriale interne des juridictions belges, pourtant évoquée *infra*, n° 375.

1173 Prés. Comm. Mechelen, 27 avril 2010, *Ann. prat. marché, propriété intellectuelle, concurrence,* 2010, p. 517. Dans cette affaire, le président considère qu'un site Web de jeux de hasard constitue un établissement de jeux de hasard que la loi définit comme « les bâtiments ou les lieux où sont exploités un ou plusieurs jeux de hasard », article 2, 3°, 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, *M.B.*, 30 décembre 1999. Pour une autre analogie entre le monde « physique » et le monde « virtuel », en matière de rémunération pour copie privée, voy. *infra*, n° 376.

1174 Par exemple, voy. *infra*, n°s 355 et 356.