Criminalité informatique

de Villenfagne, Florence

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

Publication date:
2010

Document Version
le PDF de l'éditeur

CHRONIQUE DE JURISPRUDENCE 2002-2008

Criminalité informatique

Florence de Villenfagne[1]

I. INTRODUCTION

C'est en 2001[2] que la Belgique s'est dotée d'un arsenal législatif permettant de combattre plus efficacement la criminalité informatique. Avant cette date, les cours et tribunaux pouvaient se trouver fort démunis face à des délits utilisant ou visant l'informatique. Ils n'avaient en effet que le Code pénal de 1867 et des lois spéciales (comme, entre autres, la loi du 21 mars 1991 portant réforme de certaines entreprises publiques et économiques, la loi du 14 juillet 1991 sur les pratiques du commerce, la loi « vie privée » du 8 décembre 1992, la loi du 30 juin 1994 relative aux droits d'auteur et au droit voisin, la loi du 30 juin 1994 sur la protection des programmes d'ordinateur ou encore la loi du 30 juin 1994 relative aux écoutes téléphoniques, la prise de connaissance et l'enregistrement de communications et télécommunications privées), pour agir efficacement.

Mais lors de l'application de ces textes, la question résidait souvent dans l'interprétation que l'on pouvait valablement leur donner, car très peu d'entre eux faisaient référence à une application dans un contexte électronique. La jurisprudence resta divisée sur ce sujet : certaines juridictions interprétaient les textes de façon stricte, alors que d'autres utilisaient parfois les moyens les plus originaux pour faire « entrer » les faits dans une définition existante. Les juges tentaient ainsi d'utiliser avec plus ou moins de succès (vu l'interdiction en droit pénal de l'interprétation analogique[3]) la qualification de « vol d'électricité », d'interception illégale de télécommunications, de « vol avec fausses clés » lorsqu'ils rencontraient des cas[4] qui seraient qualifiés aujourd'hui de *hacking* ou de

[1] Chercheur senior au CRID (Centre de Recherches Informatique et Droit) – FUNDP.

[2] Loi du 28 novembre 2000, *M.B.,* 3 février 2001, p. 2909.

[3] Une interprétation évolutive est cependant acceptée : « Il est permis au juge statuant en matière répressive d'appliquer la loi pénale à des faits que le législateur était dans l'impossibilité absolue de prévoir à l'époque de la promulgation de la disposition pénale, à la double condition que la volonté du législateur d'ériger des faits de cette nature en infraction soit certaine et que ces faits puissent être compris dans la définition légale de l'infraction » (Cass., 11 septembre 1990, *Pas.,* 1991, I, p. 36 et Cass., 4 mai 1988, *Pas.*, 1988, I, p. 1071).

[4] Voy., par exemple, la célèbre affaire *Bistel*. Dans cette affaire, le tribunal avait condamné, en première instance, deux individus qui s'étaient introduits de façon illicite dans le serveur informatique du premier ministre – via un mot de passe détourné – du chef de faux et usage de faux, vol d'électricité et interception illégale de télécommunications. Le tribunal correctionnel avait jugé que l'introduction frauduleuse du mot de passe constitue un écrit et, partant, un faux (Corr. Bruxelles, 8 novembre 1990, *J.T.*, 1990, p. 11). En appel, la cour avait écarté les premières préventions pour ne retenir que la dernière. En ce qui concerne la notion d'écrit, elle trancha clairement dans le sens opposé (Bruxelles, 24 juin 1991, *R.D.P.C.*, 1992, p. 340).
Voy. aussi l'affaire *ReDATtacK* : Corr. Gand, 11 décembre 2001, *Computerr.,* 2001, p. 84, note E. Kindt et E. Szafran ; *A&M,* 2001, p. 157, note B. Michaux ; *Rev. dr. pén.,* 2001, p. 97, note B. Michaux et S. Evrard.

fraude informatique. Les mêmes difficultés étaient rencontrées face à un faux commis par des moyens informatiques. Pouvait-on considérer ce faux comme un faux *en écriture* ?

La nécessité d'une clarification et de l'adoption d'une nouvelle loi se faisait pressante et il y fut répondu par la loi du 28 novembre 2000 relative à la criminalité informatique[5].

La nouvelle loi prévoit deux types d'incriminations pénales : celles qui visent à réprimer les infractions commises au moyen de l'informatique et celles visant les infractions dirigées contre le système informatique en tant que tel. Dans la première catégorie, on retrouve « la 'variante informatique' donnée à de nombreux délits classiques »[6]. De nouvelles incriminations sont prévues telles que le faux en informatique (article 210*bis* du Code pénal) et la fraude informatique (article 504*quater* du Code pénal)[7]. Dans la deuxième catégorie, sont repris les délits dits « spécifiques[8] », dirigés contre les systèmes informatiques. La loi a ainsi prévu de réprimer le *hacking* (article 550*bis* du Code pénal) et les actes de sabotage informatique (article 550*ter* du Code pénal)[9].

Le présent chapitre s'attache à analyser la jurisprudence des années 2002 jusqu'à 2008 qui applique cette nouvelle loi. Comme nous le verrons, les premières décisions prises sous l'empire de la nouvelle loi gardent les traces des interprétations anciennes dont nous parlions en introduction et montrent la difficulté qu'ont eue – et que peuvent toujours rencontrer – les juges pour qualifier les faits lorsque l'informatique est impliquée.

Avant de nous plonger dans l'étude de la jurisprudence en l'organisant par incrimination, deux remarques doivent toutefois être faites.

La première est qu'il peut y avoir de grandes similitudes « entre les conditions d'existence des différentes infractions informatiques […] qui rendent la réalisation de l'une le plus souvent connexe à d'autres »[10]. Il n'est donc pas toujours aisé de décider dans quelle section une décision doit être incluse. Nous avons fait le choix, lorsque le cas se présentait, d'analyser la décision sous le chapitre consacré à l'incrimination qui nous semblait principale en l'espèce. Un renvoi vers cette analyse sera fait dans les autres sections si cela s'avérait nécessaire.

---

5 Modifiée par la loi du 15 mai 2006, *M.B.*, 12 septembre 2006. Pour une analyse doctrinale de la loi, voy., entre autres, O. Leroux, « Criminalité informatique », in *Les infractions contre les biens*, Bruxelles, Larcier, 2008, pp. 365-453 ; E. Roger France, « Transactions électroniques et criminalité informatique : quelle répression ? », in *Aspects juridiques du paiement électronique,* tome 2, 2004, Kluwer, pp. 235 et s. ; O. Leroux, « Le faux informatique », *J.T.*, 2004, pp. 509 et s. ; Fl. 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,* 2001, pp. 65 et s. ; 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 », *R.D.P.,* 2001, pp. 611 et s. ; P. De Hert, « De wet van 28 novembre 2000 inzake informaticacriminaliteit en het materieel strafrecht : een wet die te laat komt of die er nooit had moeten komen ? », *T. Strafr.*, 2001, pp. 241 et s.

6 E. Roger France, « Transactions électroniques et criminalité informatique : quelle répression ? », in *Aspects juridiques du paiement électronique,* tome 2, 2004, Kluwer, p. 235.

7 Cette catégorie comprend également d'autres incriminations qui n'ont pas été reprises dans la loi (parce que d'autres textes les prévoyaient déjà) telles que les préventions contre les cas de port public de faux nom, de création, utilisation, conservation de matériel à caractère pédopornographique,…

8 La première catégorie reprenant les délits dits « aspécifiques ».

9 Notez que la fraude informatique pourrait aussi être rangée parmi les délits spécifiques dans la mesure où il s'agit de « l'escroquerie d'une machine ».

10 O. Leroux, note d'obs. sous Corr. Eupen (4e ch.), 15 décembre 2003, *R.D.T.I.,* 2004, liv. 19, p. 65.

Une seconde remarque est que, bien que cette chronique commence en 2002, deux décisions datant de cette période concernent des faits antérieurs à l'entrée en vigueur de la loi, nous présentons ces décisions dans une première section.

II. DÉCISIONS AVANT L'ENTRÉE EN VIGUEUR DE LA LOI BELGE SUR LA CRIMINALITÉ INFORMATIQUE

Comme nous le soulignions à l'instant, la période couverte comprend deux décisions concernant des faits antérieurs à l'entrée en vigueur de la loi. Leur analyse nous semble néanmoins intéressante, non seulement dans un souci de complétude, mais aussi parce qu'elles montrent le problème d'interprétation auquel étaient confrontés les juges avant l'entrée en vigueur de la nouvelle loi.

A. Propos racistes – *Hacking* – Ancienne loi

Le tribunal correctionnel de Bruxelles[11] fut amené à se prononcer sur un cas de **haine raciale proférée dans un forum de discussion**. Les responsables d'Infonie (modérateurs du forum) sont tout de suite intervenus lorsque les propos ont été publiés par le prévenu. Ils ont même été menacés et injuriés par celui-ci et Infonie s'est portée partie civile. La question de la responsabilité des intermédiaires ne se pose donc pas dans le cas présent.

Le tribunal a jugé qu'il s'agissait d'infractions à la loi du 30 juillet 1981 tendant à réprimer certains actes inspirés par le racisme ou la xénophobie, dans les circonstances indiquées à l'article 444 du Code pénal, ainsi qu'à l'article 1er de la loi du 23 mars 1995 tendant à réprimer la négation, la minimisation, la justification ou l'approbation du génocide commis par le régime national-socialiste allemand pendant la seconde guerre mondiale.

Mais outre cela, ce qui nous intéresse particulièrement pour notre propos, est le fait que le prévenu avait utilisé les abonnements Infonie d'autres personnes pour se connecter à Internet à leur insu, émettre ses propos et menacer les responsables d'Infonie. La nouvelle loi sur la criminalité informatique n'étant pas en vigueur au moment des faits (1997 et 1998), le tribunal jugea qu'il y avait infraction aux articles 114, § 8, 117 et 118 de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques (dispositions aujourd'hui abrogées).

B. Harcèlement – Faux de droit commun – Ancienne loi – Difficulté de qualification

Dans une autre affaire[12] dont les faits eurent lieu avant l'entrée en vigueur de la nouvelle loi, la question qui se posait en l'espèce était de savoir si, sous l'empire de l'ancienne loi, l'on pouvait considérer que la création d'une adresse internet avec un nom imaginaire pour l'utiliser à dessein de nuire, en l'occurrence pour **rédiger et publier** sur internet, **dans un groupe de discussion, deux messages attribués faussement** à une dame en insérant le numéro de téléphone de cette dernière, constituaient des faux et usage de faux de droit commun (en d'autres mots, des faux *en écriture*). Le message, invitant explicitement à prendre contact avec la dame pour des rela-

11 Corr. Bruxelles, 15 janvier 2002, inédit, publié sur www.droit-technologie.org.

12 Civ. Liège (12e ch. corr.), 18 novembre 2002, *R.D.T. I.,* 2003, pp. 95 et s., note O. Leroux.

tions sexuelles, mena à un harcèlement téléphonique de la dame par des personnes tierces qui n'étaient pas au courant du caractère faux du message publié.

Avec Olivier Leroux qui analyse en profondeur la décision liégeoise[13], nous émettons de sérieux doutes quant à la qualification de faux en écriture de droit commun[14] donnée par le tribunal. L'auteur souligne à raison que les éléments constitutifs du faux en écriture de droit commun ne sont pas réunis, en l'occurrence particulièrement l'existence d'une « écriture », elle-même constitutive de quatre éléments (écriture matérielle, étant l'expression d'une pensée, ayant un contenu juridiquement relevant et bénéficiant de la confiance collective). Y a-t-il non seulement une écriture matérielle, mais aussi tromperie de la confiance collective dans un environnement de forum de discussion à caractère sexuel où la plupart des gens se présentent sous un pseudonyme ? Comme l'auteur, nous pensons que ces conditions ne sont pas remplies et que le tribunal aurait plus opportunément condamné le prévenu sur la base d'autres incriminations telles que la protection de la vie privée, l'usurpation de fonctions, titres ou de nom, le harcèlement, ou encore les atteintes à l'honneur ou à la considération des personnes, notamment la calomnie et la diffamation.

Il est intéressant de remarquer que dans la note suivant la décision, l'auteur saisit l'occasion pour se demander si la décision aurait pu être différente si l'article 210*bis* du Code pénal (faux en informatique) avait été en vigueur au moment des faits. L'auteur épingle ici la difficulté d'interprétation d'un des éléments constitutifs du faux en informatique[15], à savoir la modification de la portée juridique des données. Il conclut ici encore, à raison, à l'inexistence du faux, mais souligne opportunément que « cette décision semble augurer des difficultés d'interprétation et d'application que différentes dispositions de la loi du 28 novembre 2000 ne vont pas manquer de susciter ». Il n'avait pas tort. Nous verrons que pour toutes les nouvelles infractions des problèmes de qualification furent rencontrés[16], qui menèrent même certains cas devant notre Cour suprême.

III. DÉCISIONS SOUS L'EMPIRE DE LA LOI BELGE DU 28 NOVEMBRE 2000

Les décisions qui suivent concernent des faits qui ont eu lieu sous l'empire de la nouvelle loi sur la criminalité informatique. Comme nous l'avons dit, certaines d'entre elles reflètent la difficulté qu'ont eue les juges à s'adapter à ce nouvel environnement criminel qu'est l'électronique – des difficultés d'interprétation étaient à prévoir et ont effectivement eu lieu.

Nous avons fait le choix d'organiser les décisions par type d'infraction : le faux en informatique (section A), la fraude informatique (section B), le *hacking* (section C) et le sabotage informatique (section D). La criminalité informatique inclut cependant également les variantes informatiques

13 O. Leroux, « Vers un premier faux informatique », note d'obs. sous Civ. Liège (12e ch. corr.), 18 novembre 2002, *R.D.T.I.*, 2003, pp. 97 et s.

14 Article 193 du Code pénal.

15 Les éléments constitutifs du faux informatique sont la réalisation d'un faux, l'introduction, la modification ou la suppression de données dans un système informatique, l'intention frauduleuse ou le dessein de nuire et la modification de la portée juridique des données.

16 Voy., par exemple, Cass. (2e ch.), 6 mai 2003, R.G. n° P.03.0366.N, *Pas.*, 2003, liv. 5-6, p. 915 ; *R.A.B.G.*, 2004, liv. 6, p. 367, note Y. Van Den Berge (cas de faux en informatique) ; Civ. Namur (ch. cons.), 7 janvier 2004, *R.D.T.I.*, 2005, liv. 22, note S. Dusollier et P.-Y. Potelle (cas de « désimlockage ») ; Cass. (2e ch.), 10 novembre 2004, R.G. n° P.04.0974.F, *Pas.*, 2004, liv. 11, p. 1771 (cas de sabotage informatique) ; Corr. Malines, 16 février 2006, *N.C.* 2007, liv. 2, p. 161 (cas d'infraction au droit de propriété intellectuelle).

de délits classiques tels que la pédopornographie sur internet, la contrefaçon de logiciels, les infractions à la législation sur les jeux de hasard en ligne… Il fut délibérément choisi de ne pas aborder cette jurisprudence ici et de se focaliser sur les nouvelles préventions introduites par la loi du 28 novembre 2000. Lorsque certains cas de cette jurisprudence nous ont tout de même semblé intéressants à relever, nous les avons rassemblés dans la section E « Autres questions d'intérêt ».

Le dernier volet de cette analyse s'attardera aux questions de procédure (section F). La loi sur la criminalité informatique a en effet mis à jour plusieurs questions épineuses de procédure liées à l'environnement informatique.

A. Le faux en informatique

1. Faux en informatique – Port public de faux nom (non) – Tentative de hacking

En 2005, une affaire fut l'occasion pour le tribunal de Termonde[17] d'appliquer l'article 210*bis* du Code pénal. Un journaliste d'investigation avait créé une fausse adresse *e-mail* au nom d'une personne tierce (E.V.M., échevin de sa commune) et envoyé un *e-mail* via cette adresse à un autre échevin de cette même commune (J.M.). Via la *Computer Crime Unit* de Termonde, l'adresse IP, puis l'identité de l'émetteur de cet *e-mail* furent trouvées. Le tribunal de Termonde jugea qu'il s'agissait d'un faux et usage de faux en informatique, soulignant qu'il y eut bien une manipulation de données juridiquement pertinentes (la modification de la portée juridique des données manipulées est un élément constitutif de l'infraction de faux en informatique). Pour qu'il y ait infraction de faux en informatique, il faut néanmoins qu'il y ait aussi un dol spécial[18]. Le tribunal en confirme l'existence en s'appuyant d'une part sur le fait que l'acte d'envoi de cet *e-mail* n'était pas purement impulsif (comme l'affirmait le prévenu), car il avait nécessité des actes préparatoires (création d'une fausse adresse *e-mail*), et d'autre part sur le fait que le prévenu avait avoué que le but de l'*e-mail* était de « provoquer E.V.M. », ce qui, selon le tribunal, suppose une intention de nuire. Le tribunal refuse cependant de considérer qu'il y a eu port public de faux nom. Il souligne tout d'abord que le caractère public n'est que relatif (seuls E.V.M. et J.M. ont eu connaissance du faux *e-mail*) et ensuite que le prévenu n'a pas eu la volonté de faire croire que E.V.M. était son véritable nom.

C'est aussi à Termonde que fut jugée, en 2007, une autre affaire[19] impliquant également la création de fausses adresses *e-mail* et de faux courriers électroniques. Un étudiant de l'Université d'Anvers avait tenté de s'introduire dans l'espace réservé aux professeurs du système informatique de l'université en envoyant au service informatique de l'université un faux *e-mail* émanant soi-disant d'un de ses professeurs. Dans cet *e-mail*, le « professeur » demandait un nouveau *log-in* et mot de passe prétextant ayant perdu les siens. Le service informatique, suspectant une tenta-

17 Corr. Dendermonde, 28 novembre 2005, *NjW,* 2006, liv. 138, p. 229, note J. Deene ; *R.A.B.G.,* 2007, liv. 6, p. 427 ; *T.G.R. – T.W.V.R.,* 2007, liv. 1, p. 57.

18 L'article 193 du Code pénal s'applique en effet également au faux en informatique (cette précision n'était pas dans le projet de loi initial mais a été ajoutée par amendement – voy. *Doc. parl.,* Chambre, 1990-2000, n° 213/02, 1). Voy. Fl. 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,* 2001, p. 65 ; *Contra :* J. Deene qui, dans la note suivant la décision (*NjW,* 2006, liv. 138, p. 231) affirme qu'un dol général suffit.

19 Corr. Dendermonde (13e ch.), 25 mai 2007, *T.G.R.,* 2007, p. 351.

tive d'intrusion, fournit alors de fausses données. Ceci lui permit d'identifier l'adresse IP du pirate qui tenta peu après – mais en vain – de s'introduire dans l'espace réservé aux professeurs du système informatique de l'université.

À nouveau le tribunal n'émet aucun doute sur l'existence d'un faux en informatique. Il conclut également à l'existence d'un dol spécial – les affirmations de l'étudiant selon lesquelles il voulait uniquement démontrer la faiblesse du système ne tenaient pas : comme dans l'affaire de 2005 expliquée plus haut, le tribunal considère que l'envoi d'un tel *e-mail* n'est pas impulsif (il faut créer la fausse adresse, puis le faux *e-mail*) ; de plus, en l'espèce, l'étudiant avait même contacté un tiers quelques jours plus tard, avec la même fausse adresse, pour le défier de pénétrer dans l'espace réservé et trouver les questions d'examen.

Le tribunal a retenu aussi les préventions d'usage de faux en informatique, de tentative de *hacking* avec la circonstance aggravante d'avoir agi avec une intention frauduleuse et d'incitation à un *hacking* externe.

2. Skimming – *Faux en informatique – Fraude informatique* – Hacking

Comme le souligne Olivier Leroux à l'occasion de l'analyse qu'il fait de la décision du tribunal correctionnel d'Eupen du 15 décembre 2003, il y a de « […] grandes similitudes entre les conditions d'existence des différentes infractions informatiques […] qui rendent la réalisation de l'une le plus souvent connexe à d'autres »[20]. Nous venons de le voir dans la décision du tribunal correctionnel de Termonde en 2007, mais c'est aussi le cas du *skimming* qui peut être qualifié de faux en informatique, mais aussi de *hacking* et de fraude informatique. Nous avons choisi de présenter les cas de *skimming* dans la section consacrée à cette dernière prévention[21].

B. La fraude informatique

1. Fraude informatique – Qualification des faits

Dans une première affaire[22] concernant **l'utilisation d'une carte de carburant volée** pour soustraire 1980,16 litres de diesel dans une pompe à essence, la chambre du conseil du tribunal de première instance d'Hasselt, par ordonnance du 18 octobre 2002, avait renvoyé les trois prévenus au tribunal correctionnel du chef de la prévention de ce que la loi définit comme une « fraude informatique[23] ». La cour d'appel d'Anvers, chambre correctionnelle, dans son arrêt du 5 février 2003 s'était néanmoins déclarée incompétente pour le motif qu'il ne s'agissait pas d'un faux en informatique (un délit), mais d'un vol avec effraction, escalade ou fausses clefs (un crime). Les « fausses clés » étant le code non attribué aux prévenus de la carte de carburant de la victime. Ce faisant, non seulement la cour d'appel se trompe sur la qualification des faits qui avait été faite par la chambre du conseil (qui visait une fraude informatique et non un faux en informatique, comme

20 O. Leroux, note d'obs. sous Corr. Eupen (4e ch.), 15 décembre 2003, *R.D.T. I.,* 2004, liv. 19, p. 65.

21 Voy. section B. La fraude informatique.

22 Cass. (2e ch.), 6 mai 2003, R.G. n° P.03.0366.N, *Pas*., 2003, liv. 5-6, p. 915 ; *R.A.B.G.,* 2004, liv. 6, p. 367, note Y. Van Den Berge.

23 Article 504*quater* du Code pénal : « Celui qui cherche à se procurer, pour lui-même ou pour autrui, avec une intention frauduleuse, un avantage économique illégal en introduisant dans un système informatique, en modifiant ou effaçant des données qui sont stockées, traitées ou transmises par un système informatique, ou en modifiant par tout moyen technologique l'utilisation normale des données dans un système informatique ».

le prétend la cour), mais de plus, sa qualification des faits (vol avec fausses clés) est empreinte des interprétations qui étaient données avant la loi sur la criminalité informatique.

En raison de la contradiction entre ces qualifications, la Cour de cassation est intervenue. Dans son arrêt du 6 mai 2003, elle confirme à juste titre la décision de la chambre du conseil en cassant l'arrêt de la cour d'appel.

En 2008, la même cour d'appel d'Anvers eut à connaître d'un autre cas de fraude informatique lié à l'utilisation d'une carte de crédit[24]. Il s'agissait cette fois de **l'utilisation frauduleuse d'une carte VISA** mise à disposition par un employeur. La carte avait été utilisée non pour des raisons professionnelles comme convenu entre employeur et employé, mais pour des raisons personnelles. En première instance les faits avaient été qualifiés de vol par un employé[25]. La cour d'appel d'Anvers souligne qu'il ne peut s'agir de vol, puisque le vol requiert la soustraction frauduleuse de biens. Les faits sont requalifiés de fraude informatique puisque des données ont été introduites dans un système informatique (le système de VISA) pour se procurer, avec une intention frauduleuse, un avantage économique illégal. La cour souligne encore qu'il n'est pas requis que les données introduites soient *inexactes*. La cour souligne que cela ne découle pas seulement du texte de l'article 504*quater* du Code pénal, mais aussi des exemples donnés dans l'exposé des motifs de la loi qui cite le fait de dépasser, avec une intention frauduleuse, la limite du crédit d'une carte de crédit, comme un exemple de fraude informatique[26].

Un autre cas concerne la pratique du «**désimlockage» de téléphones portables** – pratique consistant à déverrouiller des téléphones mobiles qui étaient électroniquement bloqués pour ne fonctionner qu'avec les cartes SIM d'un seul fournisseur de télécommunications mobiles. La décision[27] est cependant une simple décision de renvoi devant le tribunal correctionnel et, comme le soulignent S. Dusollier et P.-Y. Potelle dans leur commentaire, «l'ordonnance ne fournit pas une motivation très poussée sur les préventions pour lesquelles elle prononce le non-lieu». En ce qui nous concerne, la décision n'est pas particulièrement intéressante sauf à démontrer toute la difficulté pour les juges à comprendre et appliquer correctement cette matière complexe qu'est la criminalité informatique.

Après avoir analysé la question de la licéité du «désimlockage» en Belgique au regard des règles relatives aux offres conjointes et au droit d'auteur, le tribunal s'attache à analyser – malheureusement de façon très laconique et (trop) peu fouillée – la question de l'existence éventuelle d'un délit informatique. Dans son réquisitoire, le ministère public avait ratissé large parmi les infractions informatiques pour tenter de sanctionner la pratique du «désimlockage» (faux en informatique, *hacking*, utilisation de *hackertools*, sabotage informatique), mais n'avait pas inclus dans cette liste la fraude informatique – qui aurait pourtant peut-être pu être la prévention adéquate dans le cas d'espèce. De plus, les auteurs du commentaire soulignent à juste titre que le tribunal se trompe dans la plupart des cas sur la manière dont il applique les articles relatifs à la criminalité informatique dont il est question. La décision n'en est que moins intéressante encore.

[24] Anvers, 28 mai 2008, *T. Strafr.,* 2008, liv. 5, p. 406, note.

[25] «*loonbediendediefstal*».

[26] *Doc. parl.,* Chambre, 1999-2000, n° 213/1 et 214/1, p. 15.

[27] Civ. Namur (ch. cons.), 7 janvier 2004, *R.D.T. I.,* 2005, liv. 22, note S. Dusollier et P.-Y. Potelle.

2. Skimming – *Fraude informatique – Faux en informatique* – Hacking

Le *skimming* – copie illégale de données de la piste magnétique d'une carte de paiement – est typiquement un exemple de criminalité informatique mêlant diverses infractions connexes : le faux en informatique, la fraude informatique et le *hacking*[28].

Plusieurs décisions sanctionnant le *skimming* ont été rendues en 2004 mais sont restées inédites[29]. Nous regarderons de plus près la décision rendue par le tribunal correctionnel de Termonde le 14 mai 2007, publiée cette même année[30].

Dans plusieurs agences bancaires, les lecteurs (ouvre-porte) de cartes bancaires avaient été pourvus d'une rallonge permettant de copier la piste magnétique de la carte du client. Le code secret de celui-ci était ensuite filmé à l'aide d'une caméra miniature cachée dans une baguette collée au-dessus du terminal de retrait d'argent et peinte dans la même couleur que celui-ci. Les données ainsi filmées étaient envoyées par une connexion sans fil vers un récepteur lié à une caméra vidéo munie de mini-cassettes, le tout était caché dans une poubelle non loin de l'agence. Les données permettaient de créer de fausses cartes bancaires qui étaient ensuite utilisées à l'étranger[31] pour retirer un maximum d'argent au préjudice de la victime du *skimming*.

Il fait peu de doutes que le *skimming* constitue un faux en informatique, car la création de fausses cartes bancaires ou la copie de celles-ci est mentionnée explicitement dans les travaux préparatoires de la loi sur la criminalité informatique comme exemple de ce type d'infraction. Il s'agit cependant également de fraude informatique où l'on « cherche à se procurer, pour [soi-]même ou pour autrui, avec une intention frauduleuse, un avantage économique illégal, en introduisant dans un système informatique, en modifiant ou effaçant des données qui sont stockées, traitées ou transmises par un système informatique, ou en modifiant par tout moyen technologique l'utilisation normale des données dans un système informatique » (article 504*quater* du Code pénal). Le *skimming* constitue également un acte de *hacking* ; suite à la création de la fausse carte, les personnes poursuivies accédaient à et se maintenaient dans un système informatique en sachant qu'elles n'y étaient pas autorisées (article 550*bis* du Code pénal).

---

28 Un autre exemple de ce type de situation est le *phishing* (ou hameçonnage) – « technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance – banque, administration, etc. – afin de lui soutirer des renseignements personnels : mot de passe, numéro de carte de crédit, date de naissance, etc. C'est une forme d'attaque informatique reposant sur l'ingénierie sociale (sécurité de l'information). L'hameçonnage peut se faire par courrier électronique, par des sites Web falsifiés ou autres moyens électroniques », www.wikipedia.org.

29 Corr. Bruxelles, 6 janvier 2004, inédit ; Corr. Dendermonde, 7 juin 2004, inédit ; Corr. Brugge, 8 juin 2004, inédit, citées par E. Roger France, in *Aspects juridiques du paiement électronique*, Kluwer, 2004, pp. 239 et 244.

30 Corr. Dendermonde, 14 mai 2007, *T. Strafr.*, 2007, liv. 6, p. 403, note E. Baeyens.

31 Les fausses cartes étaient inutilisables en Belgique, car seul le contenu de la piste magnétique était copié et reporté sur la fausse carte. En Belgique, un terminal bancaire lira automatiquement la piste et la puce de toute carte bancaire belge, ce qui ne sera pas le cas à l'étranger où seule la piste sera lue.

3. Fraude informatique – Cartes bancaires

Dans la section consacrée à la qualification de fraudes informatiques[32], nous nous sommes attardés sur plusieurs décisions concernant des cartes de crédit (carte de carburant[33], carte VISA[34]), nous renvoyons à cette section pour les analyses de ces décisions.

La cour d'appel d'Anvers eut à connaître d'un autre cas de fraude informatique en 2008[35]. Il s'agissait en l'espèce de **l'utilisation frauduleuse de la carte bancaire d'un tiers** sans que celle-ci n'ait été falsifiée d'aucune manière (contrairement aux cas de *skimming* expliqués précédemment). En l'espèce, une dame, V.G., avait reçu l'autorisation d'O.C. d'utiliser la carte bancaire de ce dernier pour faire certains achats. V.G. utilisa cependant la carte pour d'autres achats, pour verser de l'argent sur son compte et celui de sa belle-sœur, ainsi que pour le paiement des dettes de sa belle-sœur. La cour jugea qu'il s'agissait bien d'une fraude informatique, peu importe que la personne ait reçu la carte et le code du titulaire même de la carte. Pour toutes les sommes allant au-delà des sommes ou achats autorisés par le titulaire, V.G. s'est procuré un avantage patrimonial illicite. La complicité de la belle-sœur ne fut retenue que pour les paiements et virements qui n'auraient pas pu avoir lieu sans son aide (en l'espèce les virements vers son compte, celui de son fils et ceux de ses créanciers).

4. Fraude informatique – Circonstance absolutoire – Parenté ou alliance

La cour d'appel de Bruxelles[36] eut à connaître d'un cas de **fraude informatique commis par le beau-fils de la victime**. Il fut jugé que la circonstance absolutoire de l'article 462 du Code pénal fondée sur la parenté ou l'alliance s'appliquait également à la fraude informatique (article 504*quater,* § 1er du Code pénal).

C. Le *hacking*[37]

Plusieurs décisions ont eu à connaître de cas de *hacking*, à savoir l'introduction et le maintien dans un système informatique sans en avoir l'habilitation nécessaire. Comme le fait le Code pénal dans son article 550*bis,* la jurisprudence différencie les cas de *hacking* interne et de *hacking* externe. Cette distinction, dont la constitutionnalité avait été mise en doute par le Conseil d'État et par une partie de la doctrine a été considérée parfaitement constitutionnelle par la Cour constitutionnelle (Cour d'arbitrage à l'époque) dans son arrêt du 24 mars 2004[38]. Il n'est donc pas contraire aux articles 10 et 11 de la Constitution que le pirate interne ne soit punissable que s'il a agi avec une intention frauduleuse ou dans le but de nuire alors que pour le pirate externe, le dol général suffit (le dol spécial étant une circonstance aggravante).

---

32 Voy. la section B.1.

33 Cass. (2e ch.), 6 mai 2003, R.G. n° P.03.0366.N, *Pas.*, 2003, liv. 5-6, p. 915 ; *R.A.B.G.,* 2004, liv. 6, p. 367, note Y. Van Den Berge.

34 Anvers, 28 mai 2008, *T. Strafr.,* 2008, liv. 5, p. 406, note.

35 Anvers, 10 septembre 2008, *N.C.*, 2009, liv. 5, p. 328, note P. Van Eecke.

36 Bruxelles (12e ch.), 12 février 2004, *Rev. dr. pén.*, 2004, liv. 6, p. 748.

37 La section présente plusieurs décisions concernant des cas de *hacking*. D'autres cas existent, mais ont été analysés dans d'autres sections. Voy. par exemple Corr. Dendermonde, 14 mai 2007, *T. Strafr.,* 2007, liv. 6, p. 403, note E. Baeyens ; Corr. Dendermonde (13e ch.), 25 mai 2007, *T.G.R.,* 2007, p. 351.

38 C.A. n° 51/2004, 24 mars 2004 (question préjudicielle), *Arr. C.A.,* 2004, liv. 2, p. 619 ; commentaire S. Vandromme, *Juristenkrant* 2004, liv. 90, p. 1.

Une première affaire fut jugée par le tribunal correctionnel d'Eupen[39]. Elle est surtout restée célèbre parce qu'elle fut considérée comme la première affaire appliquant la nouvelle loi sur la criminalité informatique. Les faits n'étaient cependant pas très compliqués et, comme le souligne Olivier Leroux dans sa note d'observation[40], ils ne permirent pas – contrairement aux espoirs de nombreux auteurs – de donner un éclairage jurisprudentiel aux zones d'ombres laissées par le texte. Olivier Leroux en profite cependant pour faire une analyse de ce qui est communément appelé *hacking* ou piratage.

Il s'agissait en l'espèce d'une **tentative d'introduction dans le système d'une société** grâce à l'utilisation d'un *hackertool* trouvé sur internet qui permet de craquer en force le mot de passe du système (essai de millions de combinaisons de caractères). Le journal de bord («*logbook*») du système de l'entreprise avait conservé les traces laissées par la tentative d'intrusion, ce qui permit de retrouver facilement l'auteur des faits (il avait utilisé sa propre connexion pour agir). Le tribunal qualifia à juste titre les faits de *tentative* de *hacking* externe – sanctionnée aussi sévèrement que le *hacking* lui-même (article 550*bis* du Code pénal). Comme déjà signalé précédemment, le fait que l'auteur de la tentative n'ait pas agi avec une intention de nuire (ce qui semblait être le cas en l'espèce, l'auteur ayant avoué qu'il voulait seulement vérifier si le système de son concurrent était aussi mal protégé que le sien – ce qui ne sembla pas être le cas, la tentative ayant échoué…) ne change en rien le fait qu'il y ait effectivement eu tentative de *hacking* externe – le dol spécial n'étant pas un élément constitutif de l'infraction, seulement une circonstance aggravante. Dans la note d'observation de H. Graux[41] au sujet de la même affaire, l'auteur souligne que la raison d'être de cette règle est que beaucoup de *hackers* ne font état de leurs *bonnes intentions* qu'après leur arrestation (ce qui fut d'ailleurs le cas dans cette affaire d'Eupen) et que la nature de ces intentions est souvent difficile à vérifier *a posteriori*. H. Graux souligne que la même philosophie est suivie aux Pays-Bas[42] où une autre différence est cependant notoire : le *hacking* n'y est punissable que lorsqu'on outrepasse une certaine sécurisation du système dans lequel on s'introduit. Cette condition n'existe pas en Belgique et aurait pu mener à des conclusions radicalement différentes dans l'affaire jugée par le tribunal correctionnel de Hasselt étudiée ci-après[43].

Dans son analyse de la décision d'Eupen, l'auteur du commentaire ajoute que les faits auraient également pu être constitutifs d'une tentative de faux en informatique, le prévenu ayant introduit de fausses données (un mot de passe détourné – c'est-à-dire un mot de passe correct mais obtenu frauduleusement et soumis au système par une personne autre que son titulaire) dans le système. Ceci satisfait à la condition matérielle du faux en informatique.

L'affaire jugée par le tribunal correctionnel de Hasselt[44] à laquelle nous venons de faire référence est la seconde affaire dans laquelle un juge dut appliquer les nouvelles dispositions du Code pénal sur la criminalité informatique. En l'espèce, une personne – par ailleurs gestionnaire de

39 Corr. Eupen (4e ch.), 15 décembre 2003, *Computerr.*, 2004, liv. 3, p. 129, note H. Graux ; *R.D.T. I.*, 2004, liv. 19, p. 61, note O. Leroux.

40 O. Leroux, note sous Corr. Eupen (4e ch.), 15 décembre 2003, *R.D.T. I.*, 2004, liv. 19, p. 62.

41 H. Graux, note sous Corr. Eupen (4e ch.), 15 décembre 2003 et Corr. Hasselt, 21 janvier 2004, *Computerr., 2004,* liv. 3, pp. 131 et s.

42 Dans l'article 138*a Wetboek van Strafrecht.*

43 Corr. Hasselt, 21 janvier 2004, *Computerr.,* 2004, liv. 3, p. 130, note H. Graux.

44 Corr. Hasselt, 21 janvier 2004, précitée.

réseau – avait remarqué que le **système de Netbanking** de la Banque DEXIA (ancienne Bacob) n'était pas sécurisé. Elle avait ainsi découvert qu'elle pouvait télécharger les listes des bénéficiaires d'autres utilisateurs du Netbanking de la banque, modifier les numéros de comptes bancaires de la liste des bénéficiaires de ces clients et remettre la liste ainsi modifiée sur leur disque dur. Lors d'un virement d'un client vers un de ses bénéficiaires, c'est le compte modifié par le pirate qui sera crédité. Pétri de bonnes intentions, ce *white hat hacker*[45] laissa une trace claire, mais subtile[46], de son passage espérant que la banque sécurise son système ; quinze jours plus tard, vu l'absence de réaction de la banque, il la prévint par *e-mail* – preuves que dans ce cas précis, le pirate n'avait aucune intention de nuire. La Banque porta plainte quelques jours plus tard.

Ici aussi, le jugement est l'occasion de rappeler que le dol spécial n'est pas un élément constitutif de l'infraction. Un deuxième point, déjà abordé précédemment, est que la loi belge ne prévoit pas qu'il faut craquer ou contourner un système de sécurité, contrairement à la loi néerlandaise. Si tel avait été le cas, le prévenu n'aurait probablement pas été condamné. Enfin, le jugement est l'occasion de souligner qu'il faut un lien de causalité entre l'infraction et le dommage. En l'espèce, la banque réclamait le remboursement des frais occasionnés pour sécuriser son système estimant qu'il s'agissait de dommages causés par le prévenu. Le tribunal déclara à juste titre que cette demande était non fondée estimant que ce « dommage » n'était pas la conséquence de l'infraction ; au contraire, grâce aux actes du prévenu, d'autres mauvais usages pourraient être évités. Le tribunal prononça d'ailleurs un jugement clément et la suspension du prononcé.

Le tribunal correctionnel de Bruxelles fut confronté à une affaire de *hacking* en 2008[47]. En l'espèce, dans un contexte de rumeur d'O.P.A. hostile, il fut décidé en haut lieu de **contrôler le contenu de l'ordinateur personnel d'un employé**. Le contenu du disque dur, bien que protégé par un mot de passe, fut analysé, puis copié. De plus, un *keylogger*[48] fut installé sur la machine dans l'intention de récolter de l'information sur l'activité de l'utilisateur de l'ordinateur (ce système, mal installé, ne fonctionna cependant pas).

Le tribunal conclut à une *infraction contre la confidentialité, l'intégrité et la disponibilité des systèmes informatiques et des données qui sont stockées, traitées ou transmises par ces systèmes* (titre IX*bis* du Code pénal), en l'occurrence à un cas de *hacking* externe. Le tribunal souligne que *les préoccupations économiques du groupe [ ] – restant en-deçà du droit au respect de la vie privée et à la confidentialité des données stockées dans l'ordinateur cible – ne peuvent en l'espèce pas constituer l'état de nécessité invoqué.*

Dans son analyse en droit de la tentative d'utilisation d'un *keylogger*, le tribunal conclut à une infraction à l'article 314*bis* du Code pénal (tentative d'interception de télécommunications).

45 Terme communément utilisé pour désigner les « cavaliers blancs » dont le but est de dénoncer les trous de sécurité ou les dysfonctionnements de systèmes, et non de nuire ou causer des dommages.

46 Le *hacker* laissa une *calling card* – la communication de la transaction mentionnait *hacked Bacob is aware of the problem*. L'intention de ce message était d'alerter le client – et la banque – d'un problème de sécurité dans le système.

47 Corr. Bruxelles (40e ch.), 8 janvier 2008, *J.T.*, 2008, liv. 6311, p. 337.

48 Il s'agit d'un logiciel mouchard. Bien connu des pirates informatiques, il renvoie vers une adresse déterminée par l'installateur du mouchard les touches de clavier utilisées par la personne qui travaille sur l'ordinateur – et donc ce que la personne est en train de faire. Cette technique est typiquement utilisée pour obtenir les mots de passe d'un utilisateur.

Pour la jurisprudence sur les questions de relation employeur-employé, nous renvoyons au chapitre « droit social » de la chronique publiée en juin 2009 dans cette même revue[49].

D. Le sabotage informatique

Sabotage informatique – Qualification des faits – Interprétation évolutive

Dans cette affaire[50], la cour d'appel de Bruxelles, chambre correctionnelle, avait qualifié des faits de **sabotage d'un programme informatique** de gestion de listes de mariage et de cartes de fidélité de *destruction volontaire d'une machine appartenant à autrui, destinée à produire, transporter ou distribuer l'énergie motrice ou à en consommer à des fins autres que purement domestiques* (article 523 du Code pénal). La Cour de cassation, bien que rappelant que l'interprétation évolutive est acceptée en droit pénal[51], a considéré que les conditions à respecter pour cette interprétation ne sont pas réunies en l'espèce et que la cour d'appel a attribué à l'article 523 une portée qu'il n'a pas.

Sans doute la cour d'appel avait-elle perdu de vue l'existence de l'article 550*ter* introduit par la loi sur la criminalité informatique qui, comme le rappelle la Cour de cassation, vient précisément combler une lacune du Code pénal qui ne sanctionnait pas encore le sabotage d'un système informatique en le rendant partiellement ou totalement inutilisable. Cet article sanctionne celui qui *dans le but de nuire, directement ou indirectement, introduit dans un système informatique, modifie ou efface des données, ou qui modifie par tout moyen technologique l'utilisation possible de données dans un système informatique.*

E. Autres questions d'intérêt

Comme le soulignait à juste titre Etienne Montero dans la partie de cette chronique de jurisprudence publiée en 2009 qu'il consacre au droit du commerce électronique et plus particulièrement dans la section relative aux responsabilités des prestataires intermédiaires[52], « le contentieux relatif aux contenus illicites sur l'internet intéresse plusieurs chapitres de la présente chronique. Il est concevable de privilégier la nature de l'atteinte […] et, dès lors, d'examiner les décisions de jurisprudence dans les parties consacrées respectivement aux libertés, au droit d'auteur, au droit des marques, etc. […] ». Nous voulons rappeler cette logique d'organisation de la présente chronique ici. Car si certaines décisions concernent des infractions liées à des programmes informatiques, elles ne seront pas nécessairement analysées dans cette partie consacrée à la criminalité informatique.

---

49 K. Rosier, « Droit social : contrôle de l'usage des technologies de l'information et de la communication dans les relations de travail », Chronique de jurisprudence en droit des technologies de l'information (2002-2008), *in R.D.T. I.*, n° 35, juin 2009, pp. 126-140.

50 Cass (2e ch.), 10 novembre 2004, R.G. n° P.04.0974.F, *Pas.*, 2004, liv. 11, p. 1771.

51 « Il est permis au juge d'appliquer la loi pénale à des faits que le législateur était dans l'impossibilité absolue de prévoir à l'époque de la promulgation de la disposition pénale à la double condition que la volonté du législateur d'ériger des faits de cette nature en infraction soit certaine et que ces faits puissent être compris dans la définition légale de l'infraction » (Cass., 10 novembre 2004).

52 « Chronique de jurisprudence en droit des technologies de l'information (2002-2008) », *R.D.T. I.*, n° 35, juin 2009, p. 21.

Ainsi en est-il, par exemple, de la décision du tribunal correctionnel de Malines[53] qui qualifie d'infraction au droit de propriété intellectuelle – et non de vol – le fait de prendre irrégulièrement copie d'un programme informatique[54]. Certaines décisions sont cependant à la marge de l'objet du présent chapitre et nous semblaient intéressantes à relever. Nous les commentons brièvement dans cette section.

1. Responsabilité des intermédiaires – Hyperliens vers des contenus à caractère pédopornographique

En 2004, la Cour de cassation[55] fut amenée à se prononcer sur la question de savoir si la publication d'un lien hypertexte – et donc non pas directement une photo, image ou autre support visuel à caractère pédopornographique – pouvait être considérée comme une infraction à l'article 383*bis,* § 1er du Code pénal.

L'article 383*bis,* § 1er du Code pénal punit « quiconque aura exposé, vendu, loué, distribué, diffusé ou remis des 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 ou les aura, en vue du commerce ou de la distribution, fabriqués ou détenus, importés ou fait importer, remis à un agent de transport ou de distribution ».

En l'espèce une personne, propriétaire du site illegalwebs.com, permettait à des tiers d'obtenir, via paiement, un mot de passe permettant d'ajouter des hyperliens sur son site web. Tous les liens du site renvoyaient vers des pages dont le contenu était de la pornographie enfantine. En première instance, le propriétaire du site fut condamné par le tribunal correctionnel de Hasselt[56] pour possession et diffusion de matériel pédopornographique. La cour d'appel d'Anvers[57] suivit le raisonnement du tribunal de Hasselt. Un pourvoi fut introduit devant la Cour de cassation qui rejeta ce dernier et souligna « qu'il y a également lieu d'entendre par exposer ou diffuser au sens de ladite disposition, l'installation sur un site web d'hyperliens vers des 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 d'âge ; »[58].

2. Légalité des peines – Application du principe aux infractions commises à l'occasion d'une « communication » « via l'infrastructure des télécommunications »

La Cour constitutionnelle[59] (à l'époque encore Cour d'arbitrage) a annulé l'article 151 de la loi-programme du 30 décembre 2001 qui modifiait l'article 111 de la loi du 21 mars 1991 portant

53 Corr. Malines, 16 février 2006, *N.C.*, 2007, liv. 2, p. 161.

54 Pour une analyse de la jurisprudence liée aux droits intellectuels, voy. la « Chronique de jurisprudence en droit des technologies de l'information (2002-2008) », coord. C. de Terwangne et S. Dusollier, *op. cit.*, pp. 41 et s.

55 Cass. (2e ch.), 3 février 2004, *R.V. c. Ministère public, Arr. Cass.*, 2004/2, p. 169, *Pas.*, 2004, p. 200 ; *A&M*, 2005/3, p. 259, *Computerr.*, 2004/5, p. 242, *R.D.T. I.*, n° 19/2004, p. 51, note F. de Patoul et I. Vereecken.

56 Corr. Hasselt (18e ch.), 1er mars 2002, inédit, R.G. n° 00392.

57 Anvers (10e ch.), 7 octobre 2003, *Computerr.*, 2004/2, p. 85, note C. De Preter.

58 En ce qui concerne la responsabilité des intermédiaires, voyez l'analyse de l'arrêt par Etienne Montero dans la partie de la Chronique de jurisprudence en droit des technologies de l'information (2002-2008), consacrée au droit du commerce électronique, *R.D.T. I.*, n° 35, juin 2009, pp. 21-23.

59 C.A. 69/2003, 14 mai 2003, inédit, publié sur www.droit-technologie.org.

réforme de certaines entreprises publiques économiques[60]. Dans sa décision, la Cour ne critique en rien l'opportunité d'adopter des mesures par lesquelles le législateur veut réagir contre les comportements abusifs constatés dans le secteur des télécommunications – secteur ayant connu récemment un développement important. La Cour estime en outre que le traitement différent des personnes qui émettent ou tentent d'émettre les communications visées en utilisant l'infrastructure des télécommunications et de celles qui le font sans utiliser cette infrastructure n'est pas discriminatoire, car fondé sur un critère objectif, celui de l'utilisation de l'infrastructure de télécommunications. Par contre, la Cour a annulé l'article sur la base du fait que l'infraction est définie en des termes trop vagues (« communications *portant atteinte au respect des lois* » ; « atteinte … *à la sécurité de l'État* », renvoi à des notions comme l'ordre public et les bonnes mœurs « qui ne peuvent constituer à elles seules la définition d'une infraction pénale sans créer une insécurité inadmissible », référence à l'offense à l'égard d'un État étranger qui « ne peut, sans plus de précision, être érigée en infraction sans attenter à la liberté de manifester des opinions »). En cela, la Cour base son annulation sur ce qu'elle estime être le non-respect du principe de légalité en matière pénale.

3. *Consultation d'*e-mails *à l'insu des destinataires – Secret des communications – Article 314*bis *du Code pénal – Prise de connaissance pendant la transmission de courrier électronique*

Le tribunal correctionnel de Leuven[61] eut à connaître d'un cas dont les faits ont eu lieu fin 2000[62] et qui ne furent jugés qu'en 2007[63].

En l'espèce, le prévenu, responsable informatique de sa société, avait pris connaissance d'*e-mails* de personnes dirigeant la société et ce, à l'insu de ces personnes.

Il s'agissait pour le tribunal de vérifier si les faits correspondaient aux préventions reprises à divers articles[64] de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques (dite « loi Belgacom ») – dont l'article 109*ter* D[65] – ainsi qu'à l'article 314*bis* du Code pénal. La question la plus complexe à traiter était de savoir dans quelle mesure l'on pouvait estimer que la prise de connaissance par le prévenu avait eu lieu « pendant la transmission » comme l'exige l'article 314*bis* du Code pénal. Le tribunal s'appuie, entre autres, sur les écrits de Paul De Hert[66] pour affirmer que lorsque, comme en l'espèce, un individu lit les *e-mails* d'autres personnes lorsque ces *e-mails* se trouvent toujours sur le serveur mail et qu'ils n'ont pas encore été demandés, télé-

60 « Nul ne peut, dans le Royaume, via l'infrastructure des télécommunications, donner ou tenter de donner des communications portant atteinte au respect des lois, à la sécurité de l'État, à l'ordre public ou aux bonnes mœurs ou constituant une offense à l'égard d'un État étranger ».

61 Corr. Leuven, 4 décembre 2007, *T. Strafr.*, 2008, liv. 3, p. 223, note L. Ceulemans.

62 Les faits ont eu lieu entre le 29 octobre et le 1er décembre 2000 (au moment de l'adoption de la nouvelle loi sur la criminalité informatique).

63 Le tribunal considéra d'ailleurs les délais d'instruction beaucoup trop longs.

64 En l'espèce, les articles 55, 68, 109*ter* D, al. 1er, 1°, 2°, 3° et 4°, 110, 114, § 2, 117 et 118.

65 Article abrogé depuis et remplacé par les articles 124 et 125 de la loi du 13 juin 2005 sur les communications électroniques.

66 P. De Hert, « Internetrechten in het bedrijf. Controle op *e-mail* en Internetgebruik in Belgisch en Europees perspectief », *A&M*, 2001, n° 1, pp. 165-167.

chargés vers la boîte *e-mail* (*mailbox)* de la personne, on peut considérer que la prise de connaissance de l'individu a été faite *pendant la transmission*. Le tribunal ajoute cependant un critère qui apporte une certaine confusion – soulignée par l'auteur du commentaire L. Ceulemans – à savoir que l'on peut considérer que l'on se trouve dans la période de transmission tant que l'*e-mail* n'a pas encore été lu par son destinataire (et a pourtant été téléchargé du serveur mail vers la boîte à messages). La décision ne vient donc pas complètement clarifier, comme espéré, le critère de *période de transmission* utilisé dans l'article 314*bis* du Code pénal. Si l'on peut en effet s'accorder avec la vision que la transmission d'un *e-mail* n'est pas entièrement terminée tant que l'*e-mail* ne se trouve pas effectivement dans la boîte à messages du destinataire, prêt à être lu, il est plus difficile de suivre le raisonnement selon lequel le parcours ne se termine qu'à l'ouverture et la lecture effective du courrier électronique[67].

F. Questions de procédure

La dernière partie de ce chapitre consacré aux décisions concernant la criminalité informatique abordera les questions de procédure. La loi du 28 novembre 2000 sur la criminalité informatique a aussi introduit un certain nombre de nouveaux articles dans le Code d'instruction criminelle : l'article 39*bis* (saisie dans un environnement informatique) ; 46*bis* (perquisition ou recherche dans un système informatique) ; 88*bis* (repérage de télécommunications ou localisation de l'origine ou de la destination de télécommunications) ; 88*ter* (extension de recherches informatiques) ; 88*quater* (obligation de collaboration) ; 90*ter* et 90*quater* (écoutes, prise de connaissance et enregistrement de communications et de télécommunications privées). Plusieurs cas de jurisprudence sont directement liés à l'interprétation et à l'application de ces articles. Nous vous les présentons ci-dessous.

*1. Écoutes téléphoniques – Nullité d'ordonnances d'écoute – Articles 90*ter *et 90*quater *du Code d'instruction criminelle*

Dans une affaire particulièrement grave[68] d'organisation criminelle menant des trafics de stupéfiants, de véhicules, d'écrans de télévision plasma, de DVD, et des opérations de blanchiment liées auxdits trafics, le problème vient de deux ordonnances du magistrat instructeur pour la mise sur écoute d'un numéro d'appel d'un des prévenus (une ordonnance originaire, et une ordonnance de prolongation). C'est l'exploitation de ces écoutes qui a permis au juge d'instruction de délivrer plusieurs mandats de perquisitions dont les résultats fructueux ont permis de procéder à l'arrestation des prévenus.

Le juge, ayant analysé scrupuleusement les conditions insérées par la loi du 30 juin 1994 *relative à la protection de la vie privée contre les écoutes, les prises de connaissance et l'enregistrement de communications et de télécommunications privées*[69] – loi qui autorise à titre exceptionnel la

67 Voy. d'autres réflexions sur le sujet par K. Rosier, « Droit social : contrôle de l'usage des technologies de l'information et de la communication dans les relations de travail », Chronique de jurisprudence en droit des technologies de l'information (2002-2008), *op. cit.*, p. 128 et note 711.

68 Corr. Bruxelles (54e ch.), 3 mai 2005, inédit, publié sur www.droit-technologie.org.

69 *M.B.*, 24 janvier 1995.

pratique d'écoutes téléphoniques moyennant le respect de garanties précises (articles 90*ter* et 90*quater* du Code d'instruction criminelle), constate la nullité des ordonnances d'écoute. Les écoutes téléphoniques avaient été autorisées par un juge d'instruction sur la base d'ordonnances motivées par des formules de pure forme ne contenant pas les indices et faits concrets permettant de recourir à la mesure d'écoute et à sa prolongation et ne respectant donc pas les prescrits du Code d'instruction criminelle en cette matière. Le juge déclare l'irrecevabilité des poursuites qui furent essentiellement basées sur les écoutes litigieuses.

Dans une autre affaire, la Cour de cassation a décidé, par un arrêt du 5 juin 2007[70], que lorsque des mesures de surveillance ont été ordonnées pour une période prenant cours avant la signature de l'ordonnance, la nullité ne touche que les mesures de surveillance préalables à cette date et n'entraîne pas la nullité de l'ensemble de l'ordonnance.

Enfin, par un arrêt du 19 juin 2007[71], la Cour souligne la différence entre la régularité d'une ordonnance d'écoute et celle de son exécution. La première étant à peine de nullité, alors que ce n'est pas le cas pour la seconde. Dès lors, l'irrégularité de l'exécution ne porte pas atteinte à la régularité de l'ordonnance même (article 90*quater* du Code d'instruction criminelle).

2. Écoutes téléphoniques – Article 90ter du Code d'instruction criminelle – Régularité des preuves

La Cour de cassation[72] analyse le cas de la prise de connaissance, faite de manière fortuite au cours de l'exécution d'une mesure d'écoute ordonnée régulièrement (dans un autre dossier) en application de l'article 90*ter* du Code d'instruction criminelle, d'une infraction ne pouvant pas nécessairement justifier la mesure d'écoute ordonnée. La Cour estime que les éléments de preuve ainsi recueillis dans un dossier autre que celui dans lequel la mesure de surveillance a été ordonnée peuvent tout de même être légalement utilisés par le procureur du Roi.

La Cour casse l'arrêt de la cour d'appel de Bruxelles, chambre des mises en accusation.

3. Extension de recherche dans un système informatique – Article 88ter du Code d'instruction criminelle

Le tribunal correctionnel de Bruxelles eut à connaître en janvier 2008[73] d'un cas d'extension de perquisition. En l'espèce, un juge d'instruction avait délivré une ordonnance de perquisition. Il n'était pas contesté que celle-ci incluait implicitement une ordonnance autorisant une recherche informatique sur les ordinateurs qui se trouvaient sur les lieux de la perquisition. Sur la base de ce mandat, les enquêteurs pouvaient procéder à l'analyse de la mémoire (disque dur,…) des ordinateurs ainsi découverts lors de la perquisition. En cela les parties se ralliaient à la « jurisprudence

70 Cass. (2e ch.), 5 juin 2007, (*S.E.M*), R.G. n° P.07.0291.N, www.cass.be ; *Pas.*, 2007, p. 1092.

71 Cass. (2e ch.), 19 juin 2007, (*K.S. c. G.O., n.v. e.a.*), R.G. n° P.07.0311.N, www.cass.be ; *Pas.*, 2007, p. 1274 ; *R.A.B.G.*, 2008, p. 438, note F. Van Volsem ; *T. Strafr.*, 2008, p. 41, note.

72 Cass. (2e ch.), 3 juin 2008, R.G. n° P.07.1517.N, www.cass.be ; *Pas.*, 2008, p. 1389.

73 Corr. Bruxelles, 10 janvier 2008, *T. Strafr.*, 2008, liv. 2, 149, note. Voy. aussi le commentaire de cette décision par Ph. Van Linthout et J. Kerkhofs : « Internetrecherche : informaticatap en netwerkzoeking, licht aan het eind van de tunnel », *T. Strafr.*, 2008, pp. 79 et s.

qui consacre l'idée que la saisie régulière d'un matériel informatique autorise les enquêteurs à procéder à l'analyse des données se trouvant stockées dans la mémoire de celui-ci »[74]. La défense estimait cependant que pour consulter des données qui ne se trouvaient pas directement sur le disque dur des ordinateurs (en l'occurrence, des données de la messagerie électronique se trouvant sur le serveur Hotmail), il fallait un mandat de perquisition supplémentaire – une ordonnance motivée prise en application de l'article 88*ter* du Code d'instruction criminelle par laquelle le juge d'instruction aurait autorisé une extension de recherche informatique depuis les ordinateurs découverts lors des perquisitions initiales.

Le juge a estimé qu'accéder aux informations sur ces comptes Hotmail constituait effectivement une extension de recherche informatique, mais que celle-ci pouvait être effectuée sans formalité supplémentaire pourvu que les conditions de l'article 88*ter,* § 1er *in fine* et § 2 soient respectées – contrôle qui doit être effectué par les juridictions d'instruction ou de fond et que le tribunal correctionnel de Bruxelles a fait dans le cas d'espèce. Cette décision fut critiquée par les auteurs du commentaire de la décision[75] et le jugement a été frappé d'appel.

La cour d'appel de Bruxelles[76] jugea au contraire que les recherches informatiques sur le serveur Hotmail nécessitaient soit un mandat de perquisition autorisant l'accès aux locaux du fournisseur de service (Hotmail), soit une ordonnance motivée sur la base de l'article 88*ter* du Code d'instruction criminelle (extension de recherche) permettant aux enquêteurs d'étendre la recherche pour accéder auxdits *e-mails*. Il ne suffisait donc pas au juge d'instruction de demander aux enquêteurs de prendre connaissance des courriers électroniques liés aux adresses par simple apostille, comme cela avait été fait.

La Cour décida cependant de ne pas écarter les retranscriptions des conversations électroniques incriminées des débats pour diverses raisons expliquées dans l'arrêt et plus généralement à la lumière et dans le respect des articles 6 de la Convention européenne des droits de l'homme et 14 du Pacte de New-York.

IV. JURISPRUDENCE DE LA COUR EUROPÉENNE DES DROITS DE L'HOMME

La Cour européenne des droits de l'homme eut à connaître de diverses affaires liées à l'informatique dont certaines peuvent être liées indirectement aux propos de la présente section – soit parce qu'elles concernent des contenus dommageables publiés sur Internet (*K.U. c. Finlande*), soit parce qu'elles concernent des problèmes de respect de la procédure dans le cadre de saisies informatiques (*Wieser And Bicos Beteiligungen Gmbh v. Austria ; Iliya Stefanov v. Bulgaria*). Toutes ces affaires ont cependant été analysées par la Cour au regard de la violation éventuelle de l'article 8 de la Convention européenne des droits de l'homme et nous renvoyons le lecteur à la section 3 du chapitre IV « Libertés » de la chronique de jurisprudence publiée en 2009 dans la présente

74 H.-D. Bosly et D. Vandermeersch, *Droit de la procédure pénale,* 4e éd., Bruges, La Charte, 2005, pp. 441 et 717.

75 Ph. Van Linthout et J. Kerkhofs, *op. cit.*

76 Bruxelles, 26 juin 2008, *T. Strafr.,* 2008, p. 467, note.

revue[77] pour une analyse de ces affaires au regard de la protection de la vie privée. Nous nous bornerons ici à présenter les questions proches des questions de criminalité informatique.

A. Confidentialité des télécommunications et protection de la vie privée – Fausse annonce à caractère sexuel sur internet – Mineur

Bien que, comme nous venons de le dire en introduction, elle soit plus directement liée à l'article 8 de la Convention européenne des droits de l'homme et la protection de la vie privée, une affaire portée devant la Cour européenne des droits de l'homme vaut la peine d'être abordée dans la présente chronique. Elle concerne le cas de la publication sur un site web de rencontres d'une annonce émanant soi-disant d'un jeune garçon de 12 ans qui serait à la recherche de relations intimes avec des garçons de son âge ou plus âgés. Il s'agit de l'affaire *K.U. c. Finlande*[78] commentée par Pierre-François Docquir dans le numéro 34/2009 de la présente revue[79]. Dans le cas d'espèce, la loi finlandaise ne permettait pas d'obliger l'éditeur du site de rencontres en ligne de coopérer pour repérer la personne qui avait mis en ligne cette annonce particulièrement dommageable. À l'époque des faits, la levée du secret des télécommunications ne pouvait être obtenue par les forces de l'ordre que dans le cadre d'un nombre déterminé d'infractions parmi lesquelles la calomnie (qualification employée devant les juridictions nationales) ne figurait pas. La Cour européenne des droits de l'homme viendra plutôt situer le débat sur le plan de la notion de la vie privée, qui « recouvre l'intégrité physique et morale de la personne »[80]. Ce débat sort quelque peu des propos de la présente partie de la chronique. Il reste qu'il est intéressant de souligner que la Cour précise le devoir qu'elle assigne à l'État : « bien que la liberté d'expression et la confidentialité des communications soient des considérations primordiales […] [elles ne peuvent] revêtir un caractère absolu et doi[vent] céder devant d'autres objectifs légitimes, tels que la prévention du désordre et du crime ou la protection des droits et libertés d'autrui.[…]. Il revient au législateur, […] de mettre en place le cadre qui permette de réconcilier les prétentions adverses qui s'affrontent dans ce contexte »[81].

L'analyse de l'auteur du commentaire est intéressante en ce qu'elle fait quelques réflexions prospectives tentant de voir comment cet arrêt pourrait « intervenir dans le débat relatif aux obligations que le législateur national ou européen devrait assigner aux fournisseurs de services sur Internet en termes de dévoilement ou de respect de l'identité des internautes »[82]. Il commente également la problématique de la confrontation des intérêts rivaux et la nécessité de « limiter au maximum les atteintes aux droits fondamentaux concurrents »[83], en l'occurrence, la vie privée et la liberté d'expression.

77 « Chronique de jurisprudence en droit des technologies de l'information (2002-2008) », *op. cit.*, p. 110.

78 Cour eur. D.H., *K.U. v. Finlande*, 2 décembre 2008, req. n° 2872/02, disponible en anglais sur www.echr.coe.int.

79 P.-F. Docquir, « Protection de l'enfance dans le carnaval numérique : l'article 8 de la C.E.D.H. impose un "devoir de démasquer" aux fournisseurs de services Internet », note d'obs. sous Cour eur. D.H., *K.U. v. Finlande*, 2 décembre 2008, *R.D.T. I.*, 2009, liv. 34, pp. 98 et s.

80 P.-F. Docquir, *op. cit.*, p. 100.

81 Traduction libre de P.-F. Docquir de *K.U. v. Finland*, § 49.

82 P.-F. Docquir, *op. cit.*, p. 101.

83 P.-F. Docquir, *op. cit.*, p. 103.

B. Recherche dans un système informatique – Avocat – Respect de la procédure – Secret professionnel et protection de la vie privée

Plusieurs affaires concernant des perquisitions et recherches informatiques dans un cabinet d'avocat ont été soumises à la Cour européenne des droits de l'homme ces dernières années.

Dans l'affaire *Wieser And Bicos Beteiligungen Gmbh v. Austria*[84], la Cour a estimé qu'il y avait violation de l'article 8 de la Convention européenne des droits de l'homme. Nous ne nous pencherons pas sur l'argumentation propre à la protection de la vie privée, mais relèverons cependant que la Cour conclut à la violation de l'article 8, entre autres, sur la base du non-respect de la procédure lorsqu'il s'est agi de saisir des documents électroniques. En l'espèce, si les règles de procédure autrichiennes avaient été respectées à la lettre lors de la saisie de documents papiers de l'avocat (présence d'un représentant du barreau, respect du secret professionnel, possibilité de sceller certains documents, rapport reprenant les documents saisis signé par le suspect à la fin de la saisie), les mêmes règles ne furent pas suivies pour les documents électroniques copiés et saisis d'autre part. Si cette saisie informatique fut bien considérée comme entrant dans le cadre de la perquisition telle qu'ordonnée par le juge, il ne fut pas accepté qu'il suffisait que l'avocat et le représentant du barreau aient eu la possibilité d'intervenir et de faire respecter la procédure lors de la perquisition informatique (argument de l'État attaqué). Il aurait fallu que la procédure ait effectivement été respectée ainsi que le secret professionnel.

Une autre question importante qui se pose dans le cadre de la saisie informatique est le respect du principe de proportionnalité. Lorsque des ordinateurs sont saisis ou que des disques sont copiés, il est en effet beaucoup plus difficile de respecter ce principe que lors d'une saisie classique. Lors d'une saisie classique, seuls les documents opportuns sont saisis. Lors d'une saisie informatique, l'on copie souvent l'entièreté d'un disque sans savoir si tous les documents trouvés vont être nécessaires à l'enquête. Dans de nombreux cas, certains fichiers ne vont être lisibles qu'après une analyse par un expert en informatique. L'on ne peut donc pas savoir à l'avance s'ils vont être nécessaires dans le cadre de l'enquête. L'affaire *Iliya Stefanov v. Bulgaria*[85] concerne précisément cette question de proportionnalité. Il s'agit, en l'espèce, d'un cas de saisie d'ordinateur dans un cabinet d'avocat, ordinateur qui fut gardé (trop) longtemps par les autorités avant d'être restitué au prévenu. La Cour souligne le non-respect du principe de proportionnalité dans ce cas (le disque aurait pu être copié et l'ordinateur rendu, ce qui aurait causé moins de préjudice au prévenu). La Cour se base, entre autres, sur ce point pour conclure ici aussi à la violation de l'article 8 de la Convention européenne des droits de l'homme.

C. Écoutes téléphoniques – Surveillance des « pagers », des *e-mails* et de l'usage d'internet – Surveillances secrètes (extrajudiciaires) – Surveillances audio et vidéo

La Cour européenne des droits de l'homme a également dû analyser de nombreuses affaires concernant des écoutes et surveillances de modes de communication électroniques. Ces affaires ont été présentées par Jean Herveg et Claire Gayrel dans la section 3 du chapitre IV « Libertés » de

[84] Cour eur. D.H., *Wieser And Bicos Beteiligungen Gmbh v. Austria,* 16 octobre 2007 disponible en anglais sur www.echr.coe.int (application n° 74336/01).

[85] Cour eur. D.H., *Iliya Stefanov v. Bulgaria*, 22 mai 2008, disponible en anglais sur www.echr.coe.int, (application n° 65755/01).

la chronique de jurisprudence publiée en 2009 dans la présente revue. Nous renvoyons le lecteur aux sous-sections i.et j. de cette section[86].

D. Bases de données génétiques policières

Ici encore, nous renvoyons à l'étude qui a été faite sur la question dans la chronique de jurisprudence publiée en 2009[87].

[86] « Chronique de jurisprudence en droit des technologies de l'information (2002-2008) », *op. cit.*, pp. 110 et s.

[87] « Chronique de jurisprudence en droit des technologies de l'information (2002-2008) », *op. cit.*, p. 115.