Corr. Eupen, (4e Ch.), 15 décembre 2003

Note d'observations d'Olivier LEROUX[1]

Min. publ. E. AG et S.H. (Me Zians) c. B.A. (Me Theisinger *loco* Kocks)

INTRUSION NON-AUTORISÉE DANS UN SYSTÈME INFORMATIQUE (*HACKING*) – TENTATIVE – INTERNET

Le prévenu a tenté en vain, grâce à son propre ordinateur et par une liaison téléphonique propre, de s'introduire avec l'aide d'un « programme Hacker » qu'il avait pu trouver sur Internet, dans les bases de données informatiques protégées de la S.A. X.

Les tentatives d'accès à un système informatique protégé d'autrui présentent clairement les éléments constitutifs de l'infraction visée à l'article 550bis, § 1er, alinéa 1er, et § 4, du Code pénal, dès lors que le prévenu était manifestement conscient de l'illégalité de son comportement.

Traduction libre de l'allemand

[...]

Motivation

a. Au plan pénal

Les 5, 6 et 13 janvier 2002, un ordinateur du système informatique de la S.A. X a enregistré un grand nombre de tentatives d'accès à des bases de données protégées, ce par l'intermédiaire d'une liaison Internet utilisant manifestement un programme transmettant à l'ordinateur, automatiquement et dans un laps de temps très court, des milliers de combinaisons de lettres et de mots, dans le but de pouvoir pénétrer dans la base de données étrangère lors de l'utilisation du bon code d'accès.

Peu de temps après le dépôt d'une plainte pénale par l'administrateur délégué de la S.A. X, le prévenu a pu, grâce à sa liaison Internet également enregistrée, être identifié comme étant à l'origine des tentatives d'intrusion dans les bases de données protégées.

Lors de sa première audition le 29 avril 2002, le prévenu a reconnu sans la moindre réserve qu'il a tenté en vain grâce à son propre ordinateur et par une liaison téléphonique propre, de s'introduire avec l'aide d'un « programme Hacker » qu'il avait pu trouver sur Internet, dans les bases de données informatiques protégées de la S.A. X.

Interrogé sur les motifs de ce comportement, le prévenu a expliqué qu'à côté de ses études de pédagogie de l'entreprise, psychologie et sociologie à la T.H. Aachen, il dirige en qualité d'indépendant une petite entreprise à Eupen, qui offre sur Internet des services analogues à ceux de la S.A. X et qu'il a voulu découvrir si les mesures de sécurité électroniques pour la protection des données de cette société sont aussi peu fiables que les siennes. C'est pourquoi il a entrepris d'autres essais auprès de quelques autres firmes qui travaillent avec des systèmes informatiques différents. Il n'a cepen-

1. Assistant en droit pénal (F.U.N.D.P.) et chercheur au C.R.I.D.

dant jamais réussi à pénétrer dans l'un de ces systèmes. Selon la citation, le prévenu ne se voit dès lors imputer aucune intention frauduleuse au sens de l'article 550*bis*, § 1er, alinéa 2, du Code pénal.

Les tentatives d'accès à un système informatique protégé d'autrui présentent toutefois clairement les éléments constitutifs de l'infraction visée à l'article 550*bis*, § 1er, alinéa 1er et § 4, du Code pénal, dès lors que le prévenu était manifestement conscient de l'illégalité de son comportement. En conséquence, la prévention mise à charge du prévenu est établie.

Vu le jeune âge du prévenu et son absence d'antécédents, ainsi que le caractère mineur de l'atteinte à l'ordre public qu'il a causée en l'espèce par son infraction, il peut être fait droit à la demande d'octroi de la suspension du prononcé de la condamnation.

Les objets saisis et déposés au greffe sous les n° ... sont à restituer au propriétaire légitime.

b. Au plan civil

La constitution de partie civile de la S.A. X inscrite au RC Eupen sous le n° ... ayant son siège social à ..., est recevable.

Même si la partie civile expose d'une façon crédible, que les vaines attaques dirigées contre son système informatique lui ont causé certains désagréments et généré du travail supplémentaire, les indemnités réclamées sont sans rapport causal concret avec le comportement fautif du prévenu.

Notamment, le prétendu travail supplémentaire de « près de quatre-vingt-six heures » n'est pas précisé de façon convaincante, ni *a fortiori* établi.

En conséquence, sous réserve d'une preuve plus concrète, le tribunal ne peut faire droit à la demande d'indemnité de cette partie civile que pour un montant provisionnel fixé, *ex æquo et bono* et au vu des désagréments concrétisés jusqu'ici, à 1 000 EUR.

Les constitutions de partie civile de Y et Z, domiciliés tous deux à ... sont recevable, mais non fondées, dans la mesure où ces parties civiles ne peuvent, en leur qualité d'administrateur ou directeur technique de la S.A. X, établir aucun dommage personnel qui serait en liaison causale avec l'infraction reprochée au prévenu.

Les parties civiles ne peuvent pas davantage faire valoir une motivation probante à l'appui de leur demande de publication du jugement dans un quotidien, ce d'autant moins que ces parties civiles ont manifestement dès avant l'audience pénale consacrée à cette affaire, suscité l'attention souhaitée des médias.

[...]

Note d'observations

Premier cas de *hacking* ou accès non-autorisé à un système informatique (article 550*bis* du Code pénal)

Cette décision était fort attendue. Depuis l'entrée en vigueur de la loi du 28 novembre 2000 relative à la criminalité informatique, au mois de février 2001, de nombreux plaideurs et commentateurs attendaient avec impatience que les juges aient enfin l'occasion de faire application de la loi et rendent leurs premiers jugements. Aussi, lorsque les médias annoncèrent l'avènement, dans la partie germano-

phone du pays, d'un jugement présenté comme le tout premier en la matière, les appétits des juristes versés aux nouvelles technologies s'aiguisèrent et leurs regards se tournèrent avec avidité vers Eupen.

Malheureusement, la lecture de ce jugement tant attendu laissa très certainement ces derniers sur leur faim et leur déception fut probablement à la hauteur de leur attente. Beaucoup de bruit pour rien, aurait-on pu dire. Car il est certain que cette décision n'a pu manquer de décevoir ceux qui espéraient y trouver une application docte de la loi apportant un éclairage jurisprudentiel capital là où le texte laissait subsister certaines zones d'ombre. Et pour cause : la décision ne dit rien, ou presque... Mais la pauvreté du cas d'espèce empêchait qu'il en fut autrement.

Les faits, une tentative de *hacking*, étaient en effet fort simples, dénués d'une réelle gravité intrinsèque et, surtout, n'étaient pas de nature à soulever d'intéressantes questions juridiques. Il ne fallait donc pas s'attendre à découvrir un jugement forgeant la jurisprudence en matière de criminalité informatique et il ne fait aucun doute que, si elle n'était la première application de la loi du 28 novembre 2000, cette décision serait passée inaperçue et n'aurait retenu l'attention de personne, si ce n'est celle des parties elles-mêmes. Mais voilà, ce jugement est le premier de la très courte histoire de cette loi et à ce titre (et à ce titre seulement...), il mérite que l'on s'y attarde, fût-ce un bref instant, pour revenir sur la notion de *hacking* ou piratage informatique.

En l'espèce, il était reproché au prévenu d'avoir tenté de s'introduire au moyen d'un programme de piratage dans une base de données stockée sur un système informatique appartenant à un de ses concurrents. Le programme utilisé par le prévenu permettait de soumettre à l'ordinateur visé des milliers de combinaisons de lettres et de mots susceptibles de constituer le code d'accès ou le mot de passe permettant de pénétrer dans la base de données convoitée. Ce type de programme, appelé *hackertool* et dont la conception, la recherche ou la mise à disposition est punie d'un emprisonnement allant de six mois à trois ans et/ou d'une amende comprise entre 26 et 100 000 EUR, est aussi facile à trouver qu'à utiliser. Internet regorge de petits manuels du parfait pirate, fournis avec mode d'emploi, en manière telle qu'une connaissance basique de l'informatique suffit pour se livrer à des tentatives de *hacking*. Ces logiciels (les plus simples d'entre eux, en tous cas) jouent avec les probabilités et soumettent à l'ordinateur pris pour cible une série de mots, de nombres ou de combinaisons de signes susceptibles, plus que d'autres, d'avoir été choisis par l'utilisateur comme codes ou mots de passe (il s'agit de listes prédéfinies de noms, prénoms, noms communs d'animaux de compagnie, des combinaisons de dates symboliques ou de noms propres inscrits dans la mémoire collective...). Au moyen de ce programme, et par trois reprises au moins, le prévenu a tenté sans jamais y parvenir de pénétrer à partir de son ordinateur personnel et via une simple connexion Internet dans le système informatique de son concurrent. Identifié grâce aux *log-books* de la machine visée (les *log-books* sont les journaux de bord des systèmes informatiques et enregistrent en continu de nombreuses données relatives aux opérations effectuées par le système informatique et notamment, lorsqu'il s'agit d'un serveur Internet, les adresses IP des visiteurs, véritables cartes de visite des internautes), le prévenu a immédiatement avoué les faits qui, à n'en pas douter, étaient constitutifs d'une tentative de *hacking*

telle que visée à l'article 550*bis* du Code pénal.

Cet article incrimine le *hacking* en tant qu'il est le fait de s'introduire ou de se maintenir dans le système informatique d'un tiers sans disposer de l'habilitation nécessaire à cette fin. La disposition distingue le *hacking* interne qui est le fait d'un individu disposant déjà d'un droit d'accès sur le système informatique visé et qui aurait excédé son autorisation, du *hacking* externe qui est celui réalisé par une personne étrangère au système pris pour cible.

En l'espèce, le prévenu ne disposant d'aucune autorisation d'accès ou de maintien dans le système informatique visé, il s'agissait d'une tentative de *hacking* externe rendue punissable par le paragraphe 4 de l'article 550*bis* qui sanctionne la tentative aussi sévèrement que le *hacking* lui-même (3 mois à un an d'emprisonnement et/ou une amende comprise entre 26 et 25 000 EUR, hors décimes additionnels). Cette pénalisation identique selon que l'infraction a été simplement tentée ou entièrement exécutée se justifiait, selon le législateur, par le mode d'exécution même de l'infraction et par la gravité objective du comportement incriminé. L'infraction de *hacking* se caractérisant par la volonté de son auteur d'accéder ou de se maintenir dans un système informatique dont l'accès lui est interdit et se réalisant précisément par l'introduction successive de données dans ce système en vue d'atteindre ce résultat, le législateur avait considéré que l'échec de la tentative, qu'elle soit consécutive à un manque de connaissances techniques ou à un défaut de chance, ne devait pas influencer la peine. La qualification de tentative de *hacking* fut donc à juste titre retenue par le ministère public et c'est sur cette base que le prévenu fut invité à se défendre devant le tribunal. C'est la prévention qui a, *in fine*, emporté sa condamnation.

Mais, outre la tentative de *hacking* externe, incontestable, il nous apparaît que les faits auraient également pu être constitutifs d'une tentative de faux informatique. En effet, le faux informatique se caractérise par la commission d'un faux en introduisant, modifiant ou supprimant des données dans un système informatique. Or, l'article 210*bis* du Code pénal qui incrimine le faux informatique prévoit en son paragraphe 3 que la simple tentative de faux sera elle aussi punie de la même façon que le faux lui-même. En l'espèce, en soumettant des milliers de possibilités à l'ordinateur visé dans le but de finalement lui soumettre le bon mot de passe permettant d'accéder aux données, le prévenu a tenté d'introduire de fausses données (en l'occurrence un mot de passe détourné) dans le système informatique attaqué. Le mot de passe détourné (c'est à dire le véritable mot de passe donnant accès aux données sécurisées mais obtenu frauduleusement et soumis au système informatique par une autre personne que par son titulaire) satisfait à la condition matérielle du faux informatique. Dans le même ordre d'idées, il est à noter également que si l'auteur des faits avait réussi à pénétrer sur le site convoité, il aurait commis un *hacking* externe (et non plus une simple tentative) mais aussi un faux informatique en introduisant dans la machine visée un mot de passe détourné. Ceci illustre les grandes similitudes entre les conditions d'existence des différentes infractions informatiques que d'aucuns avaient déjà mises en exergue et qui rendent la réalisation de l'une le plus souvent connexe à d'autres.

Quant à l'élément moral de l'infraction, le prévenu avait allégué qu'il avait agi de la sorte pour tester la fiabilité

des systèmes de sécurité auxquels son concurrent avait eu recours et pour vérifier notamment si ces systèmes étaient aussi peu fiables que ceux qu'il avait lui-même adoptés. Son expérience malheureuse lui aura au moins permis d'apprendre que son concurrent semblait avoir préféré un système de défense plus performant que le sien... Mais au-delà de l'aspect anecdotique de l'argumentation, cette défense n'est pas sans intérêt puisqu'elle met en lumière l'une des caractéristiques les plus discutées du *hacking* lors de l'élaboration de la loi au parlement, à savoir sa dimension morale que d'aucuns ont considéré trop lâche : l'infraction de *hacking* externe se réalise moyennant le simple dol général dans le chef de son auteur. Il faut mais il suffit que le pirate ait eu la connaissance et la volonté ou la simple acceptation de pénétrer sur le système interdit pour que l'infraction soit réalisée sur le plan moral. Contrairement à ce qui avait été décidé aux Pays-Bas, où le *hacking* n'est retenu qu'en cas d'accès à un système informatique ensuite du viol d'un système de sécurité avec dessein de nuire, le législateur belge a préféré s'en tenir à une conception moins restrictive et a privilégié le simple dol général comme élément moral de l'infraction, l'intention frauduleuse n'étant retenue qu'au titre de circonstance aggravante et ne devenant une condition d'existence que pour le *hacking* interne (qui suppose le dol spécial). La constitutionnalité de cette discrimination avait été mise en doute par le Conseil d'État, suivi sur ce point par une partie de la doctrine. Il ne fût dès lors pas étonnant que les plaideurs portèrent la question de cette éventuelle inconstitutionnalité devant la Cour d'arbitrage dans les tout premiers temps de la loi. Mais la haute juridiction décida récemment que la différence de traitement instituée par la loi entre le *hacker* interne et externe n'était pas inconstitutionnelle.

Enfin, on soulignera encore que l'infraction de *hacking* (ou sa tentative) est réalisée même en l'absence de tout préjudice (ce qui avait fait dire au Conseil d'État que la maladresse ou la curiosité pouvaient devenir un délit). Le dommage n'est en effet pas un élément constitutif de l'infraction mais seulement une circonstance aggravante (au même titre que la reprise des données ou l'utilisation du système attaqué). Il importe donc peu en l'espèce que la tentative ait ou non occasionné un quelconque dommage au gestionnaire du système informatique visé. Du moins sur le plan pénal. Car, comme l'illustre cette décision, les prétentions civiles des victimes pourront s'élever à des montants importants compte tenu de la nécessité pour elles, dans bien des cas, de recourir à des experts ou d'interrompre temporairement le fonctionnement d'un système.