La mauvaise réputation.
Ou quand savoir devient faire.

Christophe Espern – (Initiative EUCD.INFO)

«Dada est un microbe vierge»
Tristan Tzara

La loi pour la confiance dans l'économie numérique (LCEN) a été publiée au Journal Officiel le 22 juin 2004. Loi liberticide pour les uns, simplement imparfaite pour les autres, la LCEN a déchaîné les passions pendant plus de dix-huit mois, dans et hors hémicycle. La création d'une nouvelle responsabilité pour les intermédiaires techniques a focalisé l'attention et déjà fait couler beaucoup d'encre.[1]La réserve d'interprétation émise par le Conseil constitutionnel à ce sujet alimentera sans doute encore longtemps les chroniques juridiques. [2]

Au regard du changement que constitue l'introduction d'une justice asymétrique sur Internet,[3] et des difficultés de mise en oeuvre qui en découlent,[4] tout cela est compréhensible. Il n'en reste pas moins qu'il existe une autre disposition de la LCEN, qui fut beaucoup moins médiatisée, mais dont l'impact pourrait être encore plus important, tout du moins pour les programmeurs français. Car, si l'article 6 de la LCEN introduit une obligation pour les intermédiaires techniques de juger du caractère «manifestement illicite» d'un contenu, l'article 46 de la LCEN transforme lui un grand nombre de logiciels en armes, et fait de tout utilisateur d'informatique personnelle un peu trop curieux un présumé coupable. [5]

En effet, à la suite à une adaptation très stricte[6] de l'article 6 de la Convention sur la cybercriminalité, rédigée par le Conseil de l'Europe[7] et signée à Budapest en novembre 2001, notre code pénal héberge un nouvel article «L.123-3-1 ». Cet article prévoit que si une personne physique ou morale détient un moyen permettant de commettre une fraude informatique, « sans motif légitime », elle commet un délit pénal. Est considéré comme un moyen permettant la fraude informatique « un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés » pour commettre une fraude informatique.[8] Mais qu'est ce qu'un « motif légitime » ? Ce qui n'est pas « illégitime » certainement. Et nous ne sommes pas plus avancés.

Résultat ? La charge de la preuve vient d'être renversée. Le Ministère Public n'a plus à apporter la preuve de votre implication dans une fraude informatique pour que soyez passible d'une des peines prévues pour la fraude informatique aux articles 323-1 à 323-3 du Code pénal. En clair, il n'a plus à démontrer que vous vous êtes introduit frauduleusement dans un système de traitement automatisé de données, ou que vous avez aidé intentionnellement un tiers à le faire. Il doit simplement apporter la preuve d'une détention de moyens « spécialement adaptés ». A vous ensuite de démontrer l'existence d'un « motif légitime ». La belle affaire. Savoir devient faire. La détention à domicile d'une tronçonneuse et d'un manuel de clos-combat fait risquer coups et blessures.

Le citoyen français s'intéressant à la sécurité informatique, ayant donc sur son ordinateur quelques articles sur le sujet,[9] et détenant un ou deux codes sources permettant d'exploiter une faille de sécurité[10], peut dès lors être mis en examen, jugé puis condamné à une peine pouvant aller jusqu'à cinq ans de prison et/ou 75 000 euros d'amende, et ce, même si rien ne prouve qu'il s'est rendu coupable de fraude informatique, ou qu'il en ait jamais eu l'intention. Il suffit simplement qu'il ait eu conscience du fait qu'il détenait ces outils[11], qu'il n'ait pas de « motif légitime » convaincant, et que ces outils soit jugés « spécialement adaptés » à la fraude.

Cette mesure est censée permettre de mieux lutter contre le trafic de moyens qui engendrerait un « marché noir » des « outils de piratage »[12]. Le risque de mise en examen et de condamnation augmente donc sensiblement si l'individu en question a déjà, ne serait-ce que, discuté devant témoins avec des programmeurs condamnés pour ou soupçonnés de fraude informatique. A dire vrai, c'est mon cas. Et vous ?

Si vous ne vous sentez pas concerné par cette mesure, ou que vous ne souhaitez pas en faire les frais - ou si vous doutez qu'un juge d'instruction admette spontanément qu'un ordinateur hébergeant nmap, telnet et sadoor[13] n'est pas « spécialement adapté» pour commettre une fraude informatique, et qu'il est « légitime » que vous vous intéressiez à votre « sécurité informatique personnelle » [14] - je ne saurais trop vous conseiller de ne pas (ou de ne plus) chercher à comprendre ce qui se passe quand vous vous connectez à internet, et ce que l'on peut faire à distance de votre ordinateur, sauf si vous êtes militaire ou professionnel « accrédité» par le fournisseur du système d'exploitation vendu avec. [15]

Par prudence, je vous déconseille tout autant de rechercher des failles de sécurité dans les programmes qui s'éxecutent sur votre système, ou de les auditer pour voir si ils respectent vos données personnelles. A titre préventif, je vous déconseille également de copier sur un baladeur Apple un fichier téléchargé sur le site de la FNAC, de lire un DVD Disney avec un logiciel libre,[16] ou tout simplement de me rencontrer.

Il semble en effet que je dispose d'un savoir à double tranchant sur mon disque dur - les textes diraient « à double usage » -, que j'ai des centres d'interêts à priori suspects, et certaines fréquentations malvenues, qui font « manifestement » de moi un délinquant informatique. Comme disait l'autre, j'ai mauvaise réputation. Demain, je serai contrefacteur.[17]Faites attention, il paraît que c'est contagieux ...

---

1 « Faut-il créer un nouveau code d'erreur HTTP qui spécifie clairement le statut litigieux d'un site selon le FC [fournisseur de contenus] agissant sur notification d'un tiers ? Sans ce nouveau code d'erreur, comment avertir les visiteurs d'habitude d'un site frappé d'une décision de retrait, qui auraient téléchargé des fichiers ou copié les pages web du site, qu'ils sont receleurs de contenus illégaux ? [...] Je propose dans la série des codes de redirection HTTP, le code 306 (contenu illégal retiré temporairement sur information d'un tiers), 307 (contenu illégal retiré définitivement sur décision de justice).» - La loi pour la confiance dans l'économie numérique – N. Chazot (http://nicolas.chazot.free.fr/len.htm)

2 « Ce qui importe c'est la connaissance effective du droit, non du fait. Or, qui d'autre peut apporter à l'hébergeur la connaissance effective de l'atteinte au droit sinon le juge ? » "- Valse constitutionnelle à trois temps sur la responsabilité des intermédiaires techniques - Lionel Thoumyre, Légipresse n°214, sept 2004, p. 129

3 « Le dispositif de l'article 6 est structurellement asymétrique. [...] D'un côté une procédure directe entre personnes (physiques ou morales), de l'autre une action en justice. [...] Il est étonnant que le FC [fournisseur de contenus] ne soit pas tenu de saisir le propriétaire du contenu litigieux afin d'entendre ses arguments avant de couper la mise à disposition au public. Il est vrai que cela ressemblerait alors aux procédures contradictoires des tribunaux, or les hébergeurs ne sont pas des tribunaux.» - « La loi pour la confiance dans l'économie numérique » – N. Chazot (http://nicolas.chazot.free.fr/len.htm)

4 « L'encadrement du commerce électronique par la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique », JCP 2004, éd. G, act. 405 (« Principes généraux »)et 414 (« La publicité et les obligations souscrites par voie électronique»). C. Rojinsky et G.Teissonnière

5 « Art. 323-3-1. - Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée. »

6 Les Etats Membres n'avaient pas obligation de pénaliser la détention et pouvaient prévoir un nombre d'éléménts à détenir supérieur à « un » pour que soit engagée la responsabilité. Ces options n'ont pas été retenues par la France.

7 La Convention sur la cyber-criminalité (http://conventions.coe.int/Treaty/fr/Treaties/Html/185.htm)

8 Depuis la loi Godfrain du 5 janvier 1988, le droit pénal français sanctionne notamment (i) l'accès, (ii) le maintien, et (iii) l'entrave à un système automatisé de traitement de données lorsqu'il a un caractère frauduleux.

9 Par exemple : « Recherches de vulnérabilités par désassemblage » - N. Brulez - MISC – Mars/Avril 2004 ou « Récupérer une clé DES avec un voltmètre » - MISC – Septembre/Octobre 2003

10 Par exemple : le code assembleur du ver Sapphire exploitant une faille de sécurité dans Microsoft SQL Server. Lire « Analyse d'un ver ultra-rapide : Sapphire / Slammer » - N. Brulez / E.Filiol - MISC – Juillet / Août 2003 – Description en langage naturel de la faille de sécurité concernée : (http://www.nextgenss.com/advisories/mssql-udp.txt)

11 « Il n'est point de crime ou de délit sans intention de le commettre » - Article 121-3 - Code pénal

12 « Dans la mesure où la commission desdites infractions nécessite souvent la possession de moyens d'accès ("outils de piratage ") ou d'autres outils, il existe une forte motivation d'en acquérir à des fins délictueuses, ce qui peut déboucher sur la création d'une sorte de marché noir de la production et de la distribution de tels outils. Pour parer plus efficacement ces risques, le droit pénal devrait interdire des actes spécifiques potentiellement dangereux à la source, avant la commission des infractions visées aux articles 2 à 5. » (http://conventions.coe.int/Treaty/fr/Reports/Html/185.htm)

13 Pour en savoir plus sur ces programmes et leurs utilisations possibles, lire « Techniques d'attaque : l'art du cyber-camouflage » - Y. Fourastier - MISC – Septembre/Octobre 2003

14 D'où la précense de nombreux MISC dans votre appartement car « MISC propose des articles complets et pédagogiques afin d'anticiper au mieux les risques liés au piratage et les solutions pour y remédier, présentant pour cela des techniques offensives autant que défensives, leurs avantages et leurs limites, des facettes indissociables pour considérer tous les enjeux de la sécurité informatique ». MISC, journal « 100% sécurité informatique », est en vente libre dans tout bon kiosque - (http://www.miscmag.com/)

15 « Filiol [collaborateur à MISC et chef du laboratoire de virologie et de cryptologie de l'école militaire des transmissions] n'y va pas par quatre chemins. L'article 46 de la loi, déjà montré du doigt par les professionnels avant son adoption, «est une catastrophe...». «Je n'ai jamais vu autant de rejets face à un article de loi», dit-il, en le qualifiant sans retenue de «danger pour les intérêts et la souveraineté de l'État, qui pourrait donner des armes à nos adversaires pour qu'ils s'attaquent à notre patrimoine scientifique, industriel et universitaire». Et d'illustrer son propos: «Un gros éditeur de logiciels, disposant d'une batterie d'avocats, pourra porter atteinte à la recherche française, à des intérêts commerciaux, à une petite société très pointue qui le gênerait...» - « Quand un officier supérieur de l'armée tire à boulets rouges sur la LCEN » – JM. Manach - ZDNet (http://www.zdnet.fr/actualites/technologie/0,39020809,39156449,00.htm)

16 Avec Video-Lan par exemple, un logiciel initié et hébergé par l'Ecole Centrale de Paris (http://videolan.org) et dont les

auteurs ont été menacé par Apple au titre de l'EUCD car il diffusent un code source permettant la lecture sur un ordinateur d'une oeuvre encodée par une technologie Apple sans passer par un logiciel Apple. (http://eucd.info/lettre-rddv.pdf).

17 Voir « Le contournement de mesures techniques de protection : contrefaçon ou criminalité informatique » - I.Vaillant – eucd.info (http://eucd.info/documents/transposition-eucd-2003-06-20.pdf)