Fraude informatique et preuve : la quadrature du cercle ?

Marie Barel

Juriste spécialisée TIC/PI*, expert en sécurité de l'information et des systèmes.
Contact : marie.barel@legalis.net

Résumé Lors du SSTIC'04, nous avions laissée en suspens une question posée à l'issue de la conférence « *Honeypots*, un pot-pourri ... juridique », qui portait sur l'utilisation des traces informatiques enregistrées par le système pot de miel dans le cadre d'une poursuite judiciaire contre l'attaquant. Cette année, nous nous proposons donc de répondre de façon précise et détaillée à la question qui avait été ainsi formulée et qui nous conduira à exposer le régime de la preuve en matière de fraude informatique. Les notions qui seront abordées au cours de cette conférence seront donc les suivantes : système de liberté de la preuve en droit pénal et ses limites, question de la fiabilité des preuves numériques et difficultés de la preuve du caractère intentionnel et de l'imputabilité, problème de la loi applicable sur l'Internet.

Avertissement.- Le présent article reflète simplement l'opinion de son auteur et n'a pas valeur de consultation juridique.

* TIC = Technologies de l'Information et de la communication ; PI = Propriété intellectuelle.

Comme nous l'avions souligné au cours de notre conférence de l'année passée [SSTIC04], en l'absence de valeur de production, toute trace d'une activité sur un système pot de miel est en elle-même la preuve intrinsèque d'un accès indu qui est punissable, selon nous, sur le fondement des articles 323-1 et suivants[1] du code pénal. Ayant ainsi qualifié l'infraction (élément légal)[2], il reste encore au responsable de *honeypot* à rapporter deux éléments de preuve :

1. celui de la matérialité de l'infraction (en l'occurrence, au minimum un accès non autorisé dans le système) – on parle ici d' « élément matériel » de l'infraction ;
2. celui du caractère frauduleux de l'accès, l'intention (on parle aussi d' « élément moral » ou « psychologique » de l'infraction) étant caractérisée en matière de fraude informatique par la conscience d'avoir pénétré sans droit dans le système.

Comme nous le verrons dans nos développements, deux règles traditionnelles de procédure viennent donner à la preuve pénale une physionomie bien distincte de la preuve civile : ce sont la liberté de la preuve et la présomption d'innocence. Si les données techniques permettent normalement de faire la preuve du délit de fraude informatique, cette dernière obéissant au premier principe susvisé (1), la difficulté réside plutôt, pour les demandeurs à l'action publique (parquet, partie civile), dans l'établissement de la preuve de l'élément intentionnel et de l'imputabilité du délit (2). Enfin, s'agissant le plus souvent de « délits pluri-localisés », nous envisagerons les conséquences du principe de territorialité au regard de la détermination de la loi applicable, ce principe ayant été adopté par la plupart des Etats du monde et notamment la France (3).

1 Droit pénal et preuves matérielles informatiques : de la liberté de la preuve et de l'intime conviction

Avant-propos : il existe en droit français deux systèmes de preuve. Lorsque les moyens de preuve sont préalablement déterminés et imposés par loi – c'est le cas par exemple en matière d'actes juridiques –, la preuve est dite légale. Dans le cas contraire, elle est dite libre.C'est ce dernier système de « preuve libre » qui

[1] Pour mémoire, rappelons que ces articles, issus de la loi dite « Godfrain » du 5 janvier 1988, sont constitués de trois infractions principales : l'accès ou le maintien frauduleux dans un STAD, l'entrave au fonctionnement du système et enfin l'atteinte aux données du système. A ces infractions (dont la loi Perben II a renforcé les peines) s'ajoutent la répression autonome de l'association de malfaiteurs informatiques (art. 323-4 CP) et la nouvelle infraction d' « abus de dispositifs » introduite par la loi sur la confiance dans l'économie numérique du 21 juin 2004 (art. 323-3-1 CP). Sur cette dernière infraction, lire nos commentaires : *Article 323-3-1 du Code pénal : le cheval de Troie du législateur,* MISC 14 (juillet-août 2004), pp.14-17.

[2] Le principe de légalité, exprimé par l'adage « *nullum crimen, nulla poena sine lege* », signifie qu'une action (ou dans certains cas, une abstention) ne constitue une infraction que si un texte le prévoit et le sanctionne expressément.

s'applique aux faits juridiques dont le juge pénal a essentiellement à connaître[3], en particulier dans le domaine de la fraude informatique.

1.1 Principe de liberté de la preuve au pénal et ses limites

Suivant les termes de l'article 427 du Code de procédure pénale :

" *Hors les cas où la loi en dispose autrement, les infractions peuvent être établies* ***par tout mode de preuve*** *et le juge décide d'après son intime conviction.*
Le juge ne peut fonder sa décision que sur des preuves qui lui sont apportées au cours des débats et contradictoirement discutées devant lui. »

Ainsi, pour reprendre notre exemple de départ, conformément au principe de liberté de la preuve posé dans l'article susvisé, le responsable de *honeypot* pourra facilement, ou du moins « par tout mode », rapporter devant le juge la preuve de l'élément matériel de l'infraction constatée. A cet effet, toutes les données enregistrées sur le système sont bien recevables devant la justice, pourvu que celles-ci respectent les droits de la défense (principe du contradictoire).

Plus loin encore, quand bien même les tribunaux jugeraient que certaines preuves collectées sur les systèmes pot de miel constituent des procédés illicites ou déloyaux, des « pièges à pirates » procédant à des actes constitutifs d'interception illégale de correspondance – sur ce point, cf. nos propos sur « l'expectative raisonnable de confidentialité » des échanges *in* |SSTIC04] -, on constate que le **principe de loyauté dans l'administration de la preuve** s'apprécie différemment selon la personne concernée.

En effet, le principe de loyauté [GERGIN] qui, comme le principe de légalité[4], encadre la recherche et l'administration de la preuve, interdit la production de preuves obtenues par la ruse et le stratagème qui sont considérés comme des procédés contraires à la dignité de la Justice. Cependant, force est de souligner que la Cour de Cassation applique en la matière un traitement différencié selon qu'il s'agit de parties privées ou d'autorités publiques.

Ainsi, pour les représentants de l'ordre public, les preuves illicites et les provocations policières ne sont pas considérées comme des procédés de preuve acceptables, tandis que pour les autres, la chambre criminelle de la Cour[5] a rendu

[3] Notons cependant que, si l'on a besoin de prouver un *acte juridique* au cours d'un procès pénal, ce sont les règles de preuve attachées à l'acte qui s'appliqueront. Exemple : preuve par écrit pour un contrat entre des particuliers au-delà de 800 euros l'écrit pouvant être un écrit électronique, conformément à la loi du 13 mars 2000 ; preuve par tous moyens si la personne qui veut prouver cet acte est un tiers à l'acte ; preuve également libre pour un contrat entre commerçants).

[4] Ici, le principe de légalité (à ne pas confondre avec le contenu de l'élément légal de l'infraction défini plus haut) emporte interdiction de recourir à des moyens portant atteinte à la dignité humaine : torture (condamnation de la France dans un arrêt SEBMOUNI – CEDH, 28 juillet 1999), traitements inhumains ou dégradants (arrêt TOMASI – CEDH, 27 août 1992), ...

[5] Conformément au droit conventionnel ... : arrêt SCHENK - CEDH, 12 juillet 1988 > la Convention n'exclut pas « par principe et *in abstracto* » la recevabilité d'une

dans sa décision du 15 juin 1993, un attendu plus favorable repris dans l'affaire « SOS racisme »[6] au sujet du procédé de « *testing* » :

« *Attendu qu'aucune disposition légale ne permet aux juges répressifs d'écarter les moyens de preuve produits par les parties au seul motif qu'ils auraient été obtenus de façon illicite ou déloyale ; qu'il leur appartient seulement, en application du texte susvisé (article 427 CPP), d'en apprécier la valeur probante après les avoir soumis à la discussion contradictoire* ».

Cette position bienveillante de la Cour à l'égard des personnes privées est vivement critiquée par les auteurs[7] au regard des règles relatives à la preuve et à la théorie des droits de la défense dans le procès pénal.

Surtout, il est important de ne pas mal interpréter cette jurisprudence et de souligner qu'elle ne constitue en rien un encouragement à recourir à des procédés de preuve illicites ou déloyaux. En effet, comme le rappelle l'avocat général Louis di Guardia, à l'audience du 28 mai dans l'affaire « SOS Racisme » précitée, en droit français « *la production de la preuve est libre, d'autant plus quand elle est rapportée par un particulier qui n'a pas, au contraire des policiers et des gendarmes, à respecter le code de procédure pénale* "[8]. Il s'agit donc bien ici de non-respect de la procédure pénale, et non pas du *code pénal*, ce qui rend possible une action parallèle contre la personne privée qui recourrait à un procédé de preuve tombant sous le coup d'une incrimination...

1.2 Système de l'intime conviction et valeur probante des preuves informatiques

Les juges ne pouvant pas écarter par principe aucun moyen de preuve, il reste pour eux à déterminer non plus la recevabilité mais bien la valeur probante des preuves numériques qui auront été collectées par un système « pot de miel ».

Pour ce faire, « *le juge décide d'après son intime conviction* " (art. 427 CPP précité), tous les éléments de preuve apportés étant laissés à sa « *libre appréciation* » (ex. en matière d'aveu, art. 428 CPP). Comme Jean Pradel, éminent auteur du droit pénal et des sciences pénales, il est permis de considérer que **l'intime conviction** est l'équivalent exact du concept anglo-saxon de « *beyond reasonable doubt* » (au-delà du doute raisonnable) c'est-à-dire, selon la formule

preuve recueillie de manière illégale. Il incombe alors au tribunal de rechercher si le procès a présenté dans son ensemble un caractère équitable.

[6] Crim., 11 juin 2002 – Jurisdata n ° 01-5.559 – http ://www.courdecassation.fr/arrets/visu.cfm ?num=2073

[7] Par exemple, Emmanuel Molina, « *Réflexions critiques sur l'évolution paradoxale de la liberté de la preuve des infractions en droit français contemporain* » - RSC.2002.263 : « *La chambre criminelle ne semble bien ne pas avoir de théorie de la loyauté mais plutôt une politique caractérisée par une attitude strictement pragmatique consistant à arrêterses positions en fonction de l'appréciation des résultats pratiques qu'elle souhaite pouvoir obtenir. (...)* »

[8] http ://www.opuscitatum.com/...

de Lord Denning, que l'on a atteint un « *haut degré de probabilité* »[9], sans toutefois parvenir à une certitude.

Pour autant, la décision du juge **ne repose pas sur un simple raisonnement de type probabiliste**[10]. En effet, si l'on en admettait l'hypothèse dans le cadre d'un conflit de preuve littérale (ou preuve par écrit), le juge devrait alors considérer au regard des statistiques émises en matière d'écrit et de signature électronique, que les systèmes informatiques sur lesquels ils reposent, possèdent (au moins pour certains[11]) une force probante supérieure à celle du papier. Au contraire, conformément aux articles 1316-2 et 1316-3 du Code civil, l'écrit sur support électronique a bien la même force probante que l'écrit sur support papier et c'est le juge (et non pas les statistiques) qui détermine « par tous moyens le titre le plus vraisemblable, quel qu'en soit le support »...

Ainsi **chargés d'apprécier librement la fiabilité des preuves numériques** présentées devant eux, les tribunaux ont pu rendre, notamment dans le domaine commercial, des décisions très disparates, dont l'analyse permet néanmoins de tirer quelques enseignements :

1. lorsqu'il admet la force probante de la preuve électronique, le juge s'appuie généralement sur ***plusieurs*** **preuves concordantes**. Ainsi, dans l'affaire Crédicas[12], c'est la connaissance d'un code secret associée à la présentation d'une carte bancaire qui permet à une société de crédit de rapporter la preuve de ses créances, alors que, par ailleurs, *« il n'est allégué aucun dérèglement du système informatique, ni la perte du numéro secret par le débiteur »* ;
2. le juge (comme le législateur[13]) tend à réclamer une preuve que l'on considère généralement difficile à rapporter, à savoir la **preuve négative** de l'absence de négligence[14] ou de tout dysfonctionnement du système. Ainsi, dans une

[9] « Aujourd'hui, on identifie les personnes par empreinte digitale à 10^{-4}près ; on les met en prison pour viol à 10^{-9} près, à l'aide de leur empreinte génétique (...) » (chiffres cités par Me Bensoussan à l'occasion du Colloque « Commerce électronique et avenir des circuits de distribution » - CCIP/CREDA, 1998).

[10] En effet, si l'on admettait la preuve probabiliste, suivant laquelle la force probante d'une preuve juridique est mesurée par sa probabilité de fraude, en conséquence, une preuve serait (*ipso facto*) considérée comme juridiquement supérieure à une autre dès lors que, sur le plan technique, la probabilité de fraude est inférieure. En droit français, si la preuve probabiliste n'est pas rejetée en tant que telle (on admet bien la preuve par ADN, par empreinte digitale et d'autres tests techniques ou médico-légaux reposant sur des modèles statistiques), elle n'a simplement pas de force supérieure aux autres ...

[11] Par exemple les disques optiques numériques de technologie WORM (càd non réinscriptibles) pour l'archivage sécurisé des documents électroniques.

[12] Cass.civ.1$^{\text{ère}}$, 8 novembre 1989 – Bull. Civ. I, n ° 342 ; JCP G 1990, II, 21576, note G. Virassamy.

[13] Cf dans ce sens, les dispositions adoptées dans le cadre de la LCEN concernant la responsabilité des prestataires de services de certification...

[14] Par exemple, en matière de responsabilité des prestataires de services de certification électronique : articles 33 de la LCEN (loi n ° 2004-575 du 21 juin 2004 ; J.O n ° 143 du 22 juin 2004 page 11168).

affaire aux circonstances similaires à l'affaire Crédicas susvisée, la Cour d'appel de Paris[15] a au contraire rejeté la preuve informatique rapportée par la banque car elle ne rapportait pas la preuve de la négligence imputable au porteur de la carte volée ou bien encore la preuve de l'absence de défaillance du système de sécurité du distributeur.

Notons également, dans ces affaires, que le juge s'est plutôt appuyé sur une appréciation en forme de généralités et non pas sur une recherche effective à caractère technique.

Enfin et surtout, pour pouvoir emporter la conviction du juge, il sera utile de prendre toutes les **précautions techniques pour la capture, la conservation et l'analyse des données** susceptibles d'être présentées en justice. Si l'on reprend notre exemple des *honeypots*, le responsable s'assurera notamment de :

- multiplier les sources pour favoriser les recoupements, permettre la reconstruction des séquences d'attaque et servir, le cas échéant, de sauvegarde dans le cas où certains éléments tomberaient (informations générées au niveau du *honeypot* lui-même, enregistrement par le pare-feu de toutes les connexions entrantes et sortantes, détection et « isolement » des connexions suspectes à destination du *honeypot* par un IDS dont on sait que le nombre de faux positifs est d'autant réduit) ;
- conserver les données non pas en local (car les *logs* y sont possiblement l'objet des modifications d'un pirate et donc peu fiables) mais sur un système tiers (redirection vers une machine distante via le réseau). Le masquage de cet export n'est pas préconisé en l'espèce car l'une des première tâche de l'attaquant, selon les experts [MISC 8], est souvent de stopper les flux de type *syslogd* ou *syslog-ng*. L'enregistrement de cette attaque contre le serveur distant de sauvegarde reste malgré tout intéressante à deux points de vues : celui du retour sur expérience – recueil d'informations sur une attaque dirigée contre une machine qui, elle, est protégée - et celui de la démonstration d'une action anti-forensique, qui confortera, comme nous le verrons dans nos développements, la preuve de l'intention de l'attaquant ; bien entendu, les procédures de sauvegarde et d'archivage et en particulier les mesures de sécurité qui s'y appliquent pour empêcher ou limiter les risques de falsification ou de destruction des données, auront été préalablement documentées ;
- permettre l'analyse des données « *post-mortem* » à partie de copies fidèles et intègres (copies bit-à-bit sur des supports non réinscriptibles ou des systèmes de confiance, empreinte MD5 des « sorties »)[16] et en aucun cas

[15] CA Paris, 12 décembre 1980

[16] Notons que la mise en place de systèmes de signature électronique et/ou d'horodatage appliqués aux données collectées et analysées n'est jamais un pré requis pour garantir l'authenticité des données. Dans le même sens, on peut citer la jurisprudence américaine : « *In questioning whether the computer records were altered, manipulated or damaged, the courts have ruled in several cases that in the absence of any specific evidence, the* mere possibility *of tampering does not affect the authenticity of com-*

à partir des supports originaux[17] qui seront, le cas échéant, investigués par les autorités judiciaires ; de plus, dans le cadre de ces « investigations privées " (préliminaire généralement nécessaire à la qualification des incidents de sécurité), les auditeurs prendront soin de tenir très minutieusement des « cahiers d'opérations »[18] permettant de retracer toutes les actions effectuées, tant au moment de l'extraction des données que de leur analyse, de façon à assurer la traçabilité des opérations (possibilité de reconstruire le chemin menant à la preuve) et l'imputabilité des éventuelles modifications induites par les opérations d'analyse[19].

En définitive, par delà la problématique de la fiabilité des " preuves informatiques » à laquelle on répondra donc par l'anticipation et la mise en place de procédures sécurisées de capture, de conservation et d'analyse, les **difficultés de la preuve en matière de fraude informatique** résident encore davantage :

- soit dans la preuve du caractère intentionnel de l'accès frauduleux ;
- soit dans l'identification de l'auteur ou l'**imputabilité** de l'infraction.

(a) **Difficultés de la preuve de l' « élément moral » en matière de fraude informatique : entre faisceau d'indices, éléments circonstanciels et personnalité du prévenu**

L'accès dans un système d'information est frauduleux et donc punissable (article 323-1 du Code pénal) dès lors que celui-ci est effectué « *sans droit et en pleine connaissance de cause*". Ainsi l'intention est-elle caractérisée par la Cour d'appel de Paris dans un arrêt du 5 avril 1994...

La preuve de l'élément intentionnel (2.2) doit donc encore être rapportée pour permettre de faire tomber la présomption d'innocence, une entreprise souvent

puter evidence." United States v. Glassser, 773 F.2D 1553, 1559 (11Th cir. 1985). It further stated that « *the evidence of an air-tight security system [to prevent tampering] is not, however, a prerequisite to the admissibility of computer printouts. If such a prerequisite did exist, it would become virtually impossible to admit computer-generated records ; the party opposing admission would have to show only that a better security system was feasible"* (US Dept of Justice 145).

[17] BaBA de l'analyse forensique (*computer forensics*). De nombreuses références sur Internet...

[18] A l'image de Cliff Stoll dans sa poursuite du « coucou » [CUCKOO] !

[19] La liste des précautions avant analyse n'est absolument pas exhaustive ici, les spécialistes de l' « inforensique » préconisant par ailleurs d'autres mesures tout aussi essentielles :

récupération des données volatiles (c'est-à-dire les données qui ne peuvent être obtenues que lorsque le système est en fonctionnement) ;

enregistrement des données réseau (connexions en cours, en provenance ou à destination du système cible, au moment de l'incident) ;

conservation des informations d'identification et de configuration du système (topologie et paramètres réseau, versions des applications, utilisateurs et droits associés, partages, etc.) ainsi que des supports et de l'environnement applicatif nécessaire à la reproduction des faits ; etc. Cf. conférences sur ce thème dans le cadre de SSTIC'05...

difficile à laquelle les réseaux ajoutent encore un défi, celui de l'imputabilité (2.1).

1. **Présomption d'innocence et imputabilité : entre usurpation d'identité, rebond et « défense troyenne »**

Une fois que la ou les machines à l'origine de l'attaque (du moins en apparence) ont été identifiées, il reste encore à écarter plusieurs hypothèses qui permettraient aux propriétaires/responsables de ces machines de bénéficier d'un « doute raisonnable » du juge et de les considérer elles-mêmes comme victimes. Parmi ces hypothèses, on peut citer :

- le cas de l'usurpation : IP *spoofing*, usurpation d'adresse MAC (adresse physique d'une carte réseau), usurpation d'adresse mail ou de compte utilisateur...
- le cas d'une attaque par rebond où l'attaquant utilise des machines intermédiaires pour masquer son identité (adresse IP) ; ou bien encore,
- le cas d'une simple contamination de la machine (chevaux de Troie, *backdoor*, ...) permettant d'attester d'une perte de contrôle du contenu et/ou de l'utilisation de la machine.

Cette dernière stratégie de défense, appelée « *Trojan defence* », a été employée avec succès à différentes reprises[20], et notamment en octobre 2003, dans l'affaire ***Regina v. Caffrey*** (UK)[21].

Dans cette affaire, un jeune britannique âgé de 19 ans est accusé d'avoir lancé un déni de service distribué (DDOS) qui fait tomber plusieurs systèmes informatiques du port de Houston (Texas) en septembre 2001. La défense, qui n'a jamais contesté que l'origine de l'attaque soit bien la machine du jeune Aaron, soutient que le contrôle en a été pris par un pirate informatique utilisant un programme type cheval de Troie. Alors qu'aucun indice matériel ne vient corroborer les allégations du prévenu, au contraire, les éléments à charge s'accumulent :

[20] Ainsi :

Juillet 2003, *Regina v. Green* (UK) : placé en détention provisoire pour détention de 172 photos pédopornographiques, un Britannique est finalement acquitté suite au témoignage d'un expert qui a identifié onze Chevaux de Troie sur le PC de l'inculpé, ce qui corrobore l'hypothèse soutenue par l'avocat de la défense selon laquelle le téléchargement des fichiers litigieux a pu être effectué sans la connaissance ni la permission de l'utilisateur. Fait suite à une affaire similaire en avril 2003 pour des faits et des circonstances similaires (affaire *Regina v. Karl Schofield).*

Lire : http ://www.sophos.com/virusinfo/articles/porntrojan.html ("Man blames Trojan horse for child pornography")

[21] Lire : `http://news.zdnet.co.uk/0,39020330,39117033,00.htm` ("*Expert undermines hacking's suspect defence"*) ; `http://uk.news.yahoo.com/031028/80/ecbh4.html` ("*Hackers defence : the computer did it*") ; `http://www.sophos.com/virusinfo/articles/caffrey.html` ("*Teen hacker cleared by jury - blames other hackers for port of Houston attack.*") ; `http://news.zdnet.co.uk/internet/security/0,39020375,39117209,00.htm` (« *Trojan defence acquits British teenager*").

- une copie du script de l'attaque, comportant une dédicace à sa "petite amie Internet", Jessica, et signé d'un certain « Aaron », est saisie sur le disque dur du PC ;
- l'expert désigné ne relève aucune preuve de la compromission de la machine ni d'altération des fichiers de *logs* ;
- le prévenu appartient à un groupe appelé *Allied Haxor Elite* dont l'objectif déclaré est de mener avec la permission de ses amis des tests d'intrusion sur leurs machines ; ce faisant, l'appartenance à ce groupe préfigure un niveau de compétence suffisant pour écrire le script de l'attaque et l'exécuter.

La suspicion est forte, cependant le jury se laisse convaincre par le *leitmotiv* de la défense : « *computer did it* », et aussi la personnalité du jeune adolescent qui dit vouloir devenir un professionnel de la sécurité.

On le voit, en définitive, alors que des outils comme *Specter* (revenons-en encore une fois à notre exemple des pots de miel ϑ) proposent des options type scan de port en retour et de fichiers traces (*markers*), utiles[22] à l'identification des *machines* à l'origine de l'attaque et la traçabilité en général, une désagréable sensation revient au galop à l'évocation de ces affaires : celle d'un nouveau wagon de retard, qui redonne l'avantage à l'attaquant !

1.3 Elément intentionnel : signes discriminants du délinquant informatique ?

La "défense troyenne" met ainsi en cause non seulement l'imputabilité (qui a appuyé sur le bouton « ENTER » ?) mais aussi et surtout l'intentionnalité : si c'est bien moi qui ai appuyé sur ce bouton et ai déclenché telle attaque, l'ai-je fait intentionnellement – « en pleine connaissance de cause »[23] - ou au contraire, « à l'insu de mon plein gré » ? On pressent à nouveau toute la difficulté à démontrer le caractère intentionnel de l'acte de fraude informatique et ce n'est sans doute à nouveau que l'absence de contestation ou la réunion de plusieurs indices concordants qui permettra de faire la preuve de l'intentionnalité. On peut penser en particulier appliquer les raisonnements suivants.

D'abord, le **refus de collaborer** avec les autorités judiciaires (bien que notre droit reconnaisse tout à fait le « droit de se taire ») ne plaiderait pas, de façon naturelle, en faveur de l'innocence du prévenu qui, refusant notamment de révéler ses codes d'accès, mots de passe et autres conventions secrètes permettant d'accéder par exemple à des données chiffrées, ferait obstacle à la « manifestation de la vérité » sous prétexte de la protection d'informations privées ou confidentielles... Il apparaît comme une évidence que le prévenu qui se prétend victime doit bien au contraire soutenir les efforts de recherche de la police !

Ensuite, une **action anti-forensique,** consistant en l'effacement organisé et méthodique des traces informatiques, peut participer à démontrer la volonté du prévenu d'effacer son passage, l'effacement cohérent et complet de ces traces

[22] Légalité de ces procédés mise à part. Sur ce point : cf. [SSTIC04]
[23] CA Paris, 5 avril 1994 – *op.cit.*

étant par ailleurs une entreprise souvent difficile et nécessitant un certain niveau d'expertise.

Nous pourrions encore suggérer une analogie avec les contrats « double clic » : la pratique du consentement par « double clic » qui est issue de l'influence américaine, veut qu'en matière contractuelle, on joue sur un double critère positif (deux consentements successifs, pas d'option négative, validation obligatoire du « oui »). Ainsi, il n'y a de preuve du consentement au contrat que parce que deux clics, qui sont chacun une **action volontaire**, valent engagement.

De la même façon et par analogie, n'est-il pas raisonnable de penser que plus les **barrières techniques** franchies au cours d'une attaque sont nombreuses et robustes, plus l'intention frauduleuse (une action « sans droit et en pleine connaissance de cause ") est ainsi marquée. Si ces protections ne sont pas nécessaires à l'incrimination [SSTIC04], elles seront utiles pour remporter la conviction du juge, et ce d'autant que le niveau de compétences nécessaires est celui du prévenu ...

Enfin, et de façon plus scientifique, Megan Carney et Marc Rogers tentent d'ouvrir la voie de l'expertise technique comme support dans la détermination du caractère intentionnel dans les actes de fraudes informatiques. Alarmés eux aussi par le succès de la défense « Computer Did It », leur objectif est de définir un protocole et un modèle statistique discriminant, sur la base de différentes caractéristiques et variables systèmes, dont l'application permettrait d'acquérir le plus haut « degré de probabilité » concernant l'innocence ou la culpabilité du prévenu. Une entreprise qui en est encore à ses balbutiements (voir leur article sur ce sujet[24]) mais qui peut certainement contribuer, au même titre que la normalisation des techniques et méthodes inforensiques, à acquérir une confiance toujours plus grande dans les preuves informatiques rapportées devant les tribunaux.

2 Localisation du fait fautif et détermination de la loi applicable

Concentrés jusqu'ici sur l'exposé du régime de la preuve en droit français, force est de rappeler à présent que les infractions de fraude informatique sont généralement des **délits « pluri-localisés »**[25] : par exemple des cybercriminels hongrois entreprenant, à partir de la Russie, de s'attaquer à un système situé aux Etats-Unis, directement ou par l'intermédiaire d'un relais situé en Allemagne, au préjudice d'une victime de nationalité française... Quelle est dans ce cas la loi applicable ?

[24] Trojan Made Me Do It : A First Step in Statistical Based Computer Forensics Event Reconstruction – International Journal of Digital Evidence, Spring 2004, volume 2 Issue 3

[25] *Droit pénal international et Internet*, Jérôme Huet – Petites Affiches, 1999, n ° 224, p.39

2.1 L'Internet, « zone de non droit » ou super espace législatif ?

En supprimant toutes les frontières, l'Internet n'est pas devenu un espace « sans foi ni loi » ; au contraire, il a fait croître le droit en agissant comme un « processeur d'universalité »[26], comportant « *la particularité sans doute unique d'être soumis à toutes les lois de tous les Etats du monde* »[27].

En effet, suivant le **principe de territorialité**, la loi pénale nationale s'applique aux infractions commises sur le territoire national[28]. Or, l'application généralisée du principe de territorialité dans la plupart des Etats conduit à une situation complexe dans laquelle plusieurs lois sont applicables cumulativement.

Cette situation est d'autant favorisée que les Etats ont, en outre, le plus souvent adopté en matière de localisation du fait fautif pour les infractions dites « pluri localisées »[29], la théorie de l'ubiquité. Selon cette théorie, tant la loi du lieu de l'action (c'est-à-dire le territoire depuis lequel le délinquant a opéré ; dans notre hypothèse plus haut : la Russie), que la loi du lieu du résultat de l'infraction (autrement dit, celle où se sont produits les effets de l'infraction ; ici, les Etats-Unis) sont applicables. En matière de fraude informatique, la justice américaine en particulier, qui n'hésite pas à solliciter la coopération et l'entraide judiciaire des autres pays concernés[30], ni à engager des procédures d'extradition[31], fait ainsi montre d'une grande sévérité dans l'application du principe de territorialité.

De plus, pour terminer de conclure à une application universaliste de la loi pénale en matière de réseaux, il convient encore de considérer la victime, qui dans notre exemple est de nationalité française, saisissant naturellement les tribunaux nationaux ; en effet, ceux-ci appliqueront la « loi du *for* » (loi de l'Etat dans lequel est situé le tribunal saisi) pour conclure généralement (et parfois au prix d'une véritable dissection des infractions) à une application extensive de la loi nationale[32].

---

[26] Formule empruntée à Me Alain Bensoussan - Colloque « Commerce électronique et avenir des circuits de distribution », *op.cit.*

[27] *Les règles de droit international privé et la responsabilité délictuelle sur Internet*, Anne Cousin – Gaz. Pal. 2001, Doct. Page 575.

[28] En droit français, ce principe résulte très clairement de l'article 113-2 alinéa 1 du Code pénal : *« La loi pénale française est applicable aux infractions commises sur le territoire de la République »*, y inclus « *les espaces maritimes* (navires battant pavillon français) *et aériens* (aéronefs immatriculés en France) *qui lui sont liés* » (article 113-1 C.Pén.).

[29] Et ce bien avant le développement de l'Internet ! (ce qui nous fait dire que le droit n'est pas toujours si « en retard » sur la technique...).

[30] Par exemple : affaire USA v. Ehud Tenebaum (1998) – http ://www.cybercrime.gov/ ehudpr.htm ; affaire USA v. Gorshkov (2002) – http ://www.cybercrime.gov/gorshkov Sent.htm

[31] Par exemple : affaire USA v. Zezev (2003) – `http://www.cybercrime.gov/zezevSent.htm`

[32] En ce sens, les décisions prises par les tribunaux français dans des contextes internationaux, et dont l'affaire Yahoo ! (au sujet de la vente d'objets nazis) illustre la nouvelle théorie de l'orientation en matière de diffusion de contenus illicites sur l'Internet...

2.2 Cas d'application de la loi pénale française : pouvoir d'attraction de certaines infractions commises à l'étranger

Conformément au principe de territorialité, les articles 113-2 à 133-5 du code pénal énoncent donc les cas d'application de la loi pénale française commis sur le territoire de la République, qu'il s'agisse de l'auteur principal du crime ou délit ou de son complice[33]. Mais le code pénal prévoit également son application pour certaines **infractions commises *hors du territoire de la République* (article 113-6 à 113-12 C.Pén.).**

A cet égard, le premier critère de rattachement prévu est le **critère de nationalité**. Ainsi, en matière de fraude informatique (qui sont des délits punis de peines d'emprisonnement – article 323-1 et suivants du code pénal), la loi pénale française est applicable :

- aux infractions commises par des Français à l'étranger, sous condition de réciprocité d'incriminations (c'est-à-dire que les faits sont également punis par la législation du pays où ils ont été commis) – article 113-6 alinéa 2 ;

- aux infractions commises à l'étranger dès lors que la victime est de nationalité française au moment de l'infraction – article 133-7.

Le cas de pirates informatiques agissant depuis un navire ou à bord d'un avion se situant en dehors des espaces maritimes et aériens français (cf. définition *supra*) peut également donner lieu à application de la loi pénale française dans les cas prévus aux articles 113-11 et 133-12, et de façon inconditionnelle (quel que soit le lieu de commission de l'infraction et quand bien même la loi étrangère ne prévoirait pas d'incrimination pour ces faits), lorsqu'ils portent atteinte aux intérêts fondamentaux de la Nation[34] – article 113-10 C.Pén...

En définitive, eu égard aux statistiques de « géolocalisation » des attaquants informatiques[35], et sans vouloir méconnaître la complexité des procédures reposant sur la coopération judiciaire internationale[36] ou *d'exequatur*[37] des décisions étrangères, il n'existe sans doute aucun paradis judiciaire pour les pirates !

[33] Sous réserve de deux conditions : condition de réciprocité d'incriminations et décision définitive de la juridiction étrangère ayant statué sur le crime ou délit commis à l'étranger (article 113-5 C.Pén.).

[34] Articles 410-1 et suivants du code pénal : trahison et espionnage (ex. livraison d'informations à une puissance étrangère, sabotage) ; atteintes à la défense nationale (ex. violation du secret de la défense nationale), ...

[35] Voir par exemple : « *Honeypots : observation platforms* » – rapport d'expérimentation (2003-2004) d'Eurocom ; présenté dans le cadre du groupe de travail « SUR » organisé par l'OSSIR

[36] Ex. : délais d'exécution des commissions rogatoires internationales (CRI) qui passent ordinairement par la voie diplomatique

[37] Procédure par laquelle l'autorité judiciaire française donne l'ordre d'exécuter une décision rendue par une juridiction étrangère et qui permet donc la rendre effective.

3 Conclusion

Idem est non esse et non probari[38]. La preuve est la pierre angulaire de tout procès, la preuve informatique incontestée le Graal (quelle que soit leur localisation) des avocats, experts, policiers et autres protagonistes agissant dans le domaine de la fraude informatique.

En attendant que la science de l' « inforensique » acquiert ainsi ses lettres de noblesses et la placent au même rang que les preuves médico-légales, la lutte informatique continue de s'organiser (CERTs, *honeynets* distribués mondialement) et de s'armer progressivement en évoluant de plus en plus vers des systèmes d' « *active defense* "[39] (ex. *evil honeypots*)[40]. Les notions de légitimes défense (*self-defense*)[41], de contre-attaque (*counter strike*),de vigilance (*vigilantism*), de droit de poursuite (*hot pursuit*) ... sont mises en avant. Face à la jeunesse de ces solutions de « défense agressive » et les incertitudes juridiques qui peuvent en naître, la prudence reste néanmoins de rigueur dans ce domaine. Ainsi, par-delà la question de son admissibilité au regard du droit français, certains ont déjà pu souligner par exemple les risques de débordement de systèmes de riposte automatique mis en œuvre pour la légitime défense des biens[42]...

[38] « Ne pas être et ne pas être prouvé est tout un ».

[39] « *Active defense* », Laurent OUDOT – MISC 18, mars-avril 2005, pp.58-64

[40] *Retaliation with honeypots*, Laurent OUDOT – 5^{th} HOPE : http ://www.rstack.org/oudot/5th-hope/5thhope-oudot.pdf

[41] *Defending your right to defend : Considerations of an automated strike-back technology*, Timothy M. Mullen

[42] *Légitime défense des réseaux : modélisation et paramètres juridiques*, David Benichou et Serge Lefranc – JSSI, 10 mai 2005 (conférence organisée par l'OSSIR) ; voir aussi la présentation de Laurent Oudot, op.cit.

A De quelques définitions et abbréviations

Actes juridiques Les *actes juridiques* sont la manifestation d'une volonté accomplie *en vue de* produire des effets de droits (ex. contrat de fourniture d'accès à l'Internet).

CP Code pénal

CPP Code de Procédure pénale

Faits juridiques Les *faits juridiques* désignent tout évènement *susceptible* de produire des effets de droit (ex. falsification de signature électronique, usurpation d'adresse e-mail,...).

STAD Système de traitement automatisé de données

Références

[CUCKOO] Cliff Stoll, *The Cuckoo's Egg : tracking a spy through the Maze of Computer Espionnage* (1988) – ISBN 0743411463.

[GARGIN] T. Garé, C. Ginestet, Droit pénal Procédure pénale – Ed. Dalloz, 2004, ISBN 2-247-05576-1.

[MISC 8] *Honeypots, le piège à pirates !* – Dossier spécial, MISC Juillet-Août 2003, pp.24–61.

[SSTIC04] Marie Barel, « *Honeypots :* un pot-pourri... juridique » - SSTIC 2004, actes de la conférence >, `http://actes.sstic.org/SSTIC04/Droit_et_honeypots/SSTIC04-Barel-Droit_et_honeypots.pdf`