



UNIVERSITÉ DU
LUXEMBOURG

Master professionnel en Management de la Sécurité des Systèmes d'Information.

Année académique 2007-2008

La criminalité informatique dans l'entreprise : les aspects techniques et légaux de la preuve.

Par : Philippe JEANBAPTISTE

Responsable académique : Cyril PIERRE-BEAUSSE

Responsable local : Lucien ERNSTER

REMERCIEMENTS

Avant toute chose je tiens à remercier Monsieur Jean-Claude Asselborn, Directeur des études du Master MSSI, ses professeurs et mes condisciples pour le soutien logistique et moral qu'ils m'ont apporté pendant la période difficile de ma vie intervenue dans le cours de ces études, soutien sans lequel j'aurais probablement abandonné.

Merci également à Messieurs Thomas Wittlin et Lucien Ernster, ma hiérarchie, qui ont permis que je consacre une partie de mon temps professionnel à ce cursus.

Merci encore à Cyril Pierre-Beausse pour son travail accompli en tant que responsable académique ainsi que pour ses conseils en tant que juriste.

Merci à Madame Marie Pierre-Beausse Pinson pour sa relecture et ses commentaires.

Enfin merci à Emile Hazan, Alexandre Rosevègue, Alexandre Dulaunoy et tous ceux, amis et collègues, qui m'ont aidé et éclairé de leurs conseils ainsi qu'à tous les passionnés qui, sur Internet, n'hésitent pas à partager leurs connaissances.

Ce document intitulé « *La criminalité informatique en entreprise : les aspects légaux et techniques de la preuve.* » est mis à disposition sous les termes de la licence **Creative Commons**. Il peut être copié ou modifié, dans les conditions fixées par la licence, tant que cette note apparaîtra clairement. Les termes de la licence peuvent être consultés sur <http://creativecommons.org/about/licences>.

Cette version du document a été revue le 9 février 2010 suite à la nouvelle loi votée le 4 février 2010 et introduisant la responsabilité pénales des personnes morales.

RESUME

Le but de ce mémoire est de faire le point sur l'utilisation légale des outils de surveillance et de protection des systèmes d'information au Grand Duché de Luxembourg et de donner ainsi aux entreprises des points de référence.

Il envisage d'abord la législation applicable de près ou de loin aux fraudes informatiques en entreprise. A noter que certains aspects ont été écartés à dessein : Internet par exemple n'y est pas mentionné et mériterait à lui seul un autre mémoire.

Ensuite, une petite diversion sociologique fera le point sur la criminalité en entreprise et décrira une technique possible pour étudier les comportements des utilisateurs des systèmes d'information.

Suit un chapitre technique qui résume les moyens technologiques à notre disposition pour repérer et combattre les fraudes.

Enfin la dernière partie décrit la façon légale d'utiliser ces moyens technologiques, propose une organisation préalable et suggère un référentiel d'inforensique.

Mots clés : fraude informatique, législation, traces, surveillance, inforensique.



ABSTRACT

The goal of this work is to get the status of legal usage of control and protection tools for information systems in the Grand Duchy of Luxembourg and to give benchmarks to the enterprises confronted with the problem.

It first considers the laws applicable to information technology frauds in an enterprise. Please note that some aspects have been excluded on purpose: Internet for example could be the subject of a whole thesis.

Then follows a short sociological overview of the situation in enterprises, including a possible way of studying the behaviors of IT users.

A technical chapter will follow that summarizes technologies at our disposal for finding and fighting these frauds.

Finally, the last part describes the legal ways to use these technological tools, proposes an organization to be implemented prior to investigation and suggests a forensics guideline.

Key words: IT fraud, laws, traces, surveillance, forensics

Table des matières

I	Introduction	6
II	Chapitre premier : L'aspect légal	9
II.1	La structure de l'arsenal légal luxembourgeois	10
II.2	Les textes applicables : le Code Pénal	11
	Art. 509-1. (Loi du 14 août 2000)	11
	Art. 509-2. (Loi du 15 juillet 1993)	12
	Art. 509-3. (Loi du 14 août 2000)	12
	Art. 509-4. (Loi du 10 novembre 2006)	13
	Art. 509-5. (Loi du 14 août 2000).	13
	Art. 509-6. (Loi du 15 juillet 1993)	13
	Art. 509-7. (Loi du 15 juillet 1993)	13
II.3	La responsabilité	15
II.4	Code du Travail, Livre 2, Titre VI, Art. L. 261-1	16
II.5	La loi modifiée du 2 août 2002 sur la Protection des données à caractère personnel	16
II.6	La loi du 30 mai 2005	18
II.7	Autres considérations concernant le respect de la vie privée	19
III	Chapitre deux : La preuve	20
III.1	Les principes de la preuve	21
	La liberté de la preuve	21
	La publicité de la preuve	21
	Le doute	21
	La loyauté de la preuve	22
III.2	La charge de la preuve	22
III.3	Autres moyens de preuve	22
	La preuve testimoniale	22
	La preuve négative	22
III.4	L'élément humain et la défense troyenne	23
III.5	Fiabilité des preuves informatiques	23
III.6	Une preuve irréprochable	24
IV	Chapitre trois: la criminalité informatique dans l'entreprise	25
IV.1	L'analyse sociologique	26
IV.2	Les rapports officiels	27
IV.3	Au Grand Duché de Luxembourg	28

IV.4	L'ingénierie sociale ou l'importance du facteur humain	29
IV.5	Le honeypot comme instrument de mesure.....	30
V	Chapitre quatre: Les fraudes	33
V.1	Le dénominateur commun : les traces d'utilisation	34
V.2	Les moyens techniques de récolte des traces.....	35
	Le journal.....	35
	La récolte des traces de ce qui « n'existe plus ».....	37
	La récolte des traces de « ce qui n'existe pas ».....	40
VI	Chapitre cinq : L'application dans l'entreprise	43
VI.1	Les moyens juridiques de récolte des traces d'utilisation.....	44
	Le traitement de ces traces : contrôle ou surveillance ?	44
VI.2	Que peut-on faire ?.....	47
VI.3	Rôle du RSSI.....	50
VII	Chapitre six : L'infoforensique.....	52
VIII	Conclusions	56
IX	Glossaire	58
X	Bibliographie et références	59
XI	Annexes.....	62
XI.1	Annexe 1 : Extraits des différents arrêts dans l'affaire dite « wagner ».	63
XI.2	Annexe 2 : Demande d'autorisation préalable à la cnpd.....	67
XI.3	Annexe 3 : Copie du disque dur	69

Table des illustrations.

Figure 1	Pertes des entreprises dues aux attaques internes (Source : CSI 2007)	27
Figure 2	INTELLINX Monitoring Solution Architecture (Source : www.intellinx-sw.com)	36
Figure 3	Composition d'un disque dur (Source : Celog).....	38
Figure 4	Residuals of overwritten information on the side of magnetic disk tracks.(Source: Veeco).....	38
Figure 5	Volatilité et performances d'accès (Source : www.commentcamarche.net)	41

I Introduction

La révolution des technologies de l'information a changé radicalement la société et continuera vraisemblablement de le faire dans un avenir prévisible. Cette révolution a simplifié bien des tâches. Alors qu'initialement, seuls certains secteurs de la société avaient rationalisé leurs méthodes de travail en s'appuyant sur les technologies de l'information, il ne reste pour ainsi dire plus aucun secteur qu'elles n'aient marqué de leur empreinte. Les technologies de l'information se sont insinuées, d'une manière ou d'une autre, dans tous les aspects des activités humaines.

Les technologies de l'information se singularisent notamment par l'impact qu'elles ont eu et continueront d'avoir sur l'évolution des technologies des télécommunications. La téléphonie classique, qui a pour objet de transmettre la parole, a été gagnée de vitesse par l'échange de vastes quantités de données, qui peuvent être vocales, documentaires, musicales, photographiques et filmiques. Cet échange ne se déroule plus uniquement entre les êtres humains, mais intervient également entre êtres humains et ordinateurs et entre ordinateurs. Les connexions en mode circuit ont cédé la place à des réseaux à commutation par paquets. La question ne se pose plus de savoir si l'on peut établir une connexion directe : il suffit que les données soient saisies dans un réseau avec une adresse de destination ou mises à la disposition de tous ceux qui souhaitent y accéder.

La généralisation de l'utilisation du courrier électronique et de l'accès à une foule de sites web par l'Internet sont des exemples de cette évolution qui ont révolutionné notre société.

La facilité avec laquelle on peut avoir accès à l'information contenue dans les systèmes informatiques et la consulter a, couplée aux possibilités pratiquement illimitées d'échange et de diffusion de cette information, par delà les distances géographiques, déclenché une explosion de l'information disponible et des connaissances que l'on peut en tirer.

Ces développements ont donné lieu à des changements économiques et sociaux sans précédent, mais ils n'ont pas que des bons côtés : ils ont également fait apparaître de nouveaux types de délinquance et suscité la commission de délits classiques à l'aide des nouvelles technologies. Qui plus est, la délinquance peut avoir des conséquences de plus lourde portée que par le passé dans la mesure où elle ne se cantonne plus à un espace géographique donné et ne se soucie guère des frontières nationales. La propagation récente à travers le monde de virus informatiques dommageables témoigne bien de cette nouvelle réalité. Il importe de mettre en place des mesures techniques de protection des systèmes informatiques en même temps que des mesures juridiques de prévention et de dissuasion de la délinquance.

Les nouvelles technologies bousculent les principes juridiques existants. L'information et la communication circulent plus facilement que jamais à travers le monde. Les frontières ne peuvent plus s'y opposer. De plus en plus souvent les délinquants se trouvent dans des lieux fort éloignés de ceux où leurs actes produisent leurs effets. Or, les lois internes ne sont généralement applicables qu'à un territoire donné. Aussi les solutions aux problèmes posés relèvent-elles du droit international, ce qui nécessite l'adoption d'instruments juridiques internationaux adéquats. La présente Convention se propose de relever le défi ainsi posé, en tenant dûment compte de la nécessité de respecter les droits de l'homme dans la nouvelle société de l'information.

Rapport explicatif de la « *Convention sur la cybercriminalité* », Conseil de l'Europe, novembre 2001¹.

¹ Signée le 28 janvier 2003 mais pas encore ratifiée par le Grand Duché de Luxembourg.

Si j'ai choisi de reproduire cette introduction, c'est parce qu'il me semble que cette position prise par le Conseil de l'Europe évoque bien l'ampleur considérable de la problématique abordée ici, la réponse de notre société à une utilisation criminelle des nouvelles technologies de l'information.

Le problème n'est pas neuf : que ce soit Bonnie et Clyde utilisant la voiture à des fins de cambriolage ou la scission de l'atome utilisée pour construire une bombe, toutes les nouvelles technologies sont un jour détournées de leur but premier.

Les entreprises se trouvent donc confrontées à cette nouvelle forme de criminalité. Et comme dans toute affaire criminelle, il faut, pour prouver le délit, établir les faits et les comparer à des textes de loi : en effet, personne ne peut être poursuivi et puni si les éléments du délit ne sont pas définis par la loi. Curieuse situation dans laquelle se retrouvent technologies de pointe et lois poussiéreuses (certaines datant du 19^e siècle)...

Dans le cadre de mon métier –la sécurité de l'information- cette problématique est omni présente car, comme je le répéterai, ce n'est pas parce que la technologie permet tout que nous pouvons, nous, tout nous permettre.

Cette préoccupation est renforcée du fait que les métiers dans les entreprises ont tendance à se spécialiser jusqu'à en devenir très pointus. Dès lors, peut-on demander à un administrateur de réseau informatique de connaître la Code Pénal ainsi que les diverses lois régulièrement votées ou amendées ? Je ne le pense pas.

C'est ce qui m'a amené à faire le choix de ce sujet de mémoire : la personne en charge de la sécurité de l'information – donnons lui le nom de RSSI² – a, dans l'exercice de son métier, une obligation de moyens³. Il lui faut donc connaître ces moyens. J'espère donc que ce travail se révélera être utile pour les praticiens.

Vous ne trouverez pas ici de grandes descriptions technologiques : d'autres le font beaucoup mieux que moi et il existe de nombreux ouvrages détaillés et très spécialisés. De plus, en faisant cela, je retomberais dans la problématique du responsable informatique qui n'a guère le temps de s'embrasser de considérations légales. Enfin, cette technologie évolue si vite que ce qui est utile aujourd'hui ne le sera peut-être plus demain. J'ai donc préféré cerner les possibilités techniques qui s'offrent aux entreprises dans le contexte d'une fraude et leurs donner les pistes à suivre pour l'évaluer et la prouver de manière légale.

Je n'ai pas non plus abordé le rôle de la police qui dispose de prérogatives plus étendues que le chef d'entreprise et qui est tenue de respecter les procédures du Code d'instruction criminelle.

Après avoir commencé à identifier et lister les délits rendus possible par l'utilisation des technologies de l'information, je me suis rendu compte qu'elles étaient non seulement nombreuses mais en fait comparables aux délits non informatiques. En fait, ces délits ne sont pas virtuels, l'informatique n'étant qu'un moyen de les commettre. Tous ces délits sont bien réels : intrusion, vol, usurpation, détournements, ...

² Responsable de la Sécurité des Systèmes d'Information.

³ On peut, sous certaines conditions bien définies, y ajouter l'obligation de résultat.

Aidé en cela par différents cours du cursus du Master MSSSI, je me suis mis à rechercher les différents textes qui pourraient servir de base légale pour investiguer, qualifier et prouver un délit. Merci de noter que, sauf autrement précisé, il s'agit de la législation luxembourgeoise.

Et comme tous les délits, ils laissent des traces. C'est à ces traces que je me suis attaché pour étudier la manière de les collecter et les traiter d'une manière légale et dans le respect des personnes.

Ensuite je me suis attaché à condenser le tout en proposant des procédures préventives et réactives qui devraient aider les entreprises à réagir dans le cadre d'une fraude commise par son personnel. Mais nous verrons que les possibilités sont restreintes.

Enfin, je termine par suggérer un référentiel inforensique basé sur les pratiques généralement acceptées dans le milieu des investigateurs et de la justice.

Je n'ai pas voulu oublier le RSSI et c'est en quelques lignes que je décris le rôle qui devrait être le sien dans tout le processus de prévention et de réaction face aux fraudes potentielles dans son entreprise.

II Chapitre premier : L'aspect légal

« nullum crimen sine lege, nulla poena sine lege praevia »

Ce chapitre reprend quelques textes légaux qui fournissent une base légale pour qualifier et punir les délits considérés par ce travail.

En majeure partie, il reprend les textes luxembourgeois du Code pénal et du Code du travail, des extraits de certaines lois ainsi que des jurisprudences luxembourgeoises. A ceux-ci viennent s'ajouter quelques références extérieures.

Comme mentionné dans l'introduction, la criminalité informatique comprend nombres de fraudes et délits ce qui suppose que la liste des textes ci-dessous n'est probablement pas exhaustive.

II.1 LA STRUCTURE DE L'ARSENAL LEGAL LUXEMBOURGEOIS

Le Code Pénal date du 16 juin 1879 et est entré en vigueur le 15 octobre de la même année. Depuis, il a été largement modifié par les différentes lois.

Les articles traitant de la fraude informatiques ont été introduits dans ce Code Pénal par les lois successives du 15 juillet 1993, 14 août 2000 et 10 novembre 2006.

La « Convention sur la cybercriminalité » du Conseil de l'Europe⁴ a été adoptée le 23 novembre 2001 à Budapest mais, il faut le noter, n'a pas encore été ratifiée à ce jour (mars 2008) par le Grand Duché de Luxembourg. Cette Convention est le premier instrument international abordant la répression des infractions commises via l'Internet et d'autres réseaux informatiques, et traite en particulier des infractions portant atteinte au droit d'auteur, de la fraude liée à l'informatique, de la pornographie enfantine, ainsi que des infractions liées à la sécurité des réseaux. Elle prévoit également une série de procédures, notamment concernant la perquisition de réseaux informatiques et l'interception de communications électroniques. Son principal objectif est de poursuivre *"une politique pénale commune destinée à protéger la société contre le cyber crime, notamment par l'adoption d'une législation appropriée et la stimulation de la coopération internationale"*.

Avec la loi du 2 août 2002 modifiée 27 juillet 2007, le Grand Duché s'est doté d'un outil de protection des données à caractère personnel. Cette loi fait partie des textes les plus importants auxquels il sera fait référence ici car elle a en effet vocation à s'appliquer *« au traitement automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données contenues ou appelées à figurer dans un fichier [...] »*

Le 24 février 2005, le Conseil de l'union européenne a adopté une décision cadre visant à *« renforcer la coopération entre les autorités judiciaires et les autres autorités compétentes, notamment la police et les autres services spécialisés chargés de l'application de la loi dans les États membres, grâce à un rapprochement de leurs règles pénales réprimant les attaques contre les systèmes d'information. »*⁵

⁴ <http://conventions.coe.int>

⁵ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:069:0067:0071:FR:PDF>

II.2 LES TEXTES APPLICABLES : LE CODE PENAL

Le principe de légalité « *nullum crimen sine lege, nulla poena sine lege praevia* » implique qu'il n'y a pas délit si les éléments constitutifs de l'infraction et la peine encourue ne sont pas définis par la loi. Le Code Pénal et les lois spéciales (par exemple la loi du 2 août 2002) définissent ainsi les comportements susceptibles de constituer une infraction pénale, ainsi que les peines applicables.

Avec l'évolution galopante des technologies –de l'information ou autres- les lois répressives ne peuvent pas toujours appréhender l'ensemble des comportements nuisibles ou dangereux pour la société. Cela est impossible. Or, un tribunal est tenu à une interprétation stricte des textes et ne peut sanctionner un comportement déviant en l'absence de texte.

L'exemple le plus parlant est celui du courrier : quelle différence y a-t-il entre une lettre envoyée par la Poste et un courrier électronique ? Mis à part les moyens utilisés pour l'envoi, il n'y en a pas : ces deux courriers ont la même finalité et doivent donc être protégés de même manière. C'est la raison pour laquelle les tribunaux répressifs doivent se livrer à une interprétation téléologique⁶ des textes⁷ pour autant qu'ils ne détournent pas le texte et/ou ne s'éloignent pas d'une interprétation stricte des textes, garante de la liberté des citoyens.

Un tribunal répressif ne peut évidemment punir qu'un délit qui a été prouvé. La preuve s'articule autour de deux éléments importants :

- L'élément matériel (p.ex. l'accès)
- L'élément humain (p.ex. l'intention)

C'est notamment sous l'angle de ces deux éléments que les textes répressifs qui suivent sont analysés.

Art. 509-1. (Loi du 14 août 2000)

Quiconque, frauduleusement, aura accédé ou se sera maintenu dans tout ou partie d'un système de traitement ou de transmission automatisé de données sera puni d'un emprisonnement de deux mois à deux ans et d'une amende de 500 euros à 25.000 euros ou de l'une de ces deux peines.

Lorsqu'il en sera résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, l'emprisonnement sera de quatre mois à deux ans et l'amende de 1.250 euros à 25.000 euros.

« *frauduleusement* » : provient du mot fraude : « Acte de mauvaise foi accompli en contrevenant à la loi ou aux règlements et nuisant aux droits d'autrui » (Le Petit Larousse)

« *frauduleusement, aura accédé ou se sera maintenu* » Cette phrase est d'une importance primordiale. En effet, s'il est généralement compris que l'accès obtenu par une attaque informatique venant de l'extérieur est frauduleux, il est moins connu que l'accès autorisé à un système n'implique pas nécessairement que le maintien dans ce système soit régulier.

⁶ La *téléologie* (du grec télos –but- et logos -discours) est l'étude de la finalité.

⁷ MOES, René. Cours Master MSSI, *Notes de procédure pénale*.

En effet, il est possible que quelqu'un accède à un système par erreur. Dans ce cas ce quelqu'un doit « sortir » du système dès qu'il a pris conscience que son maintien n'est pas légitime, sans quoi cela pourra être considéré comme frauduleux au regard du texte sus mentionné. On peut également envisager le cas où un utilisateur autorisé à un système ne pourrait s'y maintenir pour effectuer d'autres tâches que celles pour lesquelles un accès lui a été accordé. Que pourrait-on dire d'un ancien employé à qui on a oublié de retirer ses droits d'accès et qui continue à accéder au système? Il faut donc en déduire que l'accès ou le maintien indépendamment de tout résultat dommageable relatif aux données du système sont pénalement répréhensibles !

« *la suppression ou la modification de données* » Le fait de supprimer ou de modifier des données constitue une circonstance aggravante de l'infraction d'accès ou de maintien frauduleux.

« *une altération du fonctionnement de ce système* » constitue également une aggravation de l'infraction d'accès ou de maintien frauduleux. Il est important ici de comprendre la portée du mot « *altération* » qui est selon le Petit Larousse « *l'action d'altérer, de changer la nature de quelque chose ou l'état d'une situation* ». La définition du verbe altérer est encore plus imagée : « *Changer, modifier en mal [...], détériorer, dégrader, troubler* ». On aura donc égard au caractère substantiel de la modification apportée au fonctionnement du système.

Art. 509-2. (Loi du 15 juillet 1993)

Quiconque aura, intentionnellement et au mépris des droits d'autrui, entravé ou faussé le fonctionnement d'un système de traitement ou de transmission automatisé de données sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 1.250 euros à 12.500 euros ou de l'une de ces deux peines.
--

A première vue, « *entravé ou faussé le fonctionnement d'un système* » pourrait signifier la même chose que « *une altération du fonctionnement de ce système* » présenté dans l'article précédent. Pourtant ici l'action frauduleuse n'est pas liée à l'accès : on peut donc se voir reprocher d'avoir entravé le fonctionnement d'un système sans y avoir accédé !

La loi présente ainsi un champs d'application étendu permettant d'appréhender les divers comportements de piratage informatique indépendamment les uns des autres.

Art. 509-3. (Loi du 14 août 2000)

Quiconque aura, intentionnellement et au mépris des droits d'autrui, directement ou indirectement, introduit des données dans un système de traitement ou de transmission automatisé ou supprimé ou modifié les données qu'il contient ou leurs modes de traitement ou de transmission, sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 1.250 euros à 12.500 euros ou de l'une de ces deux peines.

« *intentionnellement* » : le deuxième élément de la preuve, l'élément humain, appelé également moral, intentionnel. Et comme tous aspects humains, celui qui posera le plus de problèmes dans le déroulement d'une affaire de criminalité informatique. L'intention est donc l'autre élément constitutif de l'infraction en sus de l'élément matériel. Cet élément doit être prouvé tout comme l'élément matériel. Le plus souvent cette preuve sera déduite des faits.

« *introduit [...] ou supprimé ou modifié les données* » Si on le compare avec l'article 509-1, cet article ne parle pas d'accès ni de maintien. La différence est importante puisqu'elle permet

d'appréhender des comportements différents comme la modification, l'injection ou l'effacement.

Art. 509-4. (Loi du 10 novembre 2006)

Lorsque dans les cas visés aux articles 509-1 à 509-3, il y a eu transfert d'argent ou de valeur monétaire, causant ainsi une perte de propriété à un tiers dans un but de procurer un avantage économique à la personne qui commet l'infraction ou à une tierce personne, la peine encourue sera un emprisonnement de quatre mois à cinq ans et une amende de 1.250 euros à 30.000 euros. Encourront les mêmes peines, ceux qui auront fabriqué, reçu, obtenu, détenu, vendu ou cédé à un tiers des logiciels ayant pour objet de rendre possible une infraction visée à l'alinéa qui précède.

« *transfert d'argent ou de valeur monétaire* » Ceci constitue une circonstance aggravante des infractions considérées par les précédents articles. Les peines encourues sont en effet plus lourdes.

« *ceux qui auront fabriqué, reçu, obtenu, détenu, vendu ou cédé à un tiers des logiciels ayant pour objet de rendre possible une infraction* » Ceci est une incrimination de la complicité par fourniture de moyens en l'occurrence un logiciel et non du hardware. Le complice est puni aussi sévèrement que l'auteur lui-même.

A noter enfin que ceci ne s'applique que dans le contexte d'un transfert d'argent ou de valeur monétaire.

Art. 509-5. (Loi du 14 août 2000).

Abrogé

Art. 509-6. (Loi du 15 juillet 1993)

La tentative des délits prévus par les articles 509-1 à 509-5 est punie des mêmes peines que le délit lui-même.

Il faut faire une différence entre l'acte préparatoire qui n'est pas pénalement répréhensible et le commencement d'exécution qui caractérise la tentative punissable. Avoir en sa possession des moyens permettant une intrusion ne constitue donc pas une tentative.

Art. 509-7. (Loi du 15 juillet 1993)

Quiconque aura participé à une association formée ou à une entente établie en vue de la préparation, concrétisée par un ou plusieurs faits matériels, d'une ou de plusieurs infractions prévues par les articles 509-1 à 509-5 sera puni des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

« *association formée ou à une entente* » Il s'agit ici de punir l'association de malfaiteurs, en ce compris les individus qui auraient agi en amont de l'infraction. Un spectre très large donc.

Dispositions complémentaires du Code Pénal.

Les articles suivant sont également utiles dans la lutte contre la criminalité informatique.

Art. 196. (Loi du 14 août 2000) : L'incrimination générale du faux.

Seront punies de réclusion de cinq à dix ans les autres personnes qui auront commis un faux en écritures authentiques et publiques, et toutes personnes qui auront commis un faux en écritures de commerce, de banque ou en écritures privées, en ce compris les actes sous seing privé électronique, soit par fausses signatures, soit par contrefaçon ou altération d'écritures ou de signatures, soit par fabrication de conventions, dispositions, obligations ou décharges, ou par leur insertion après coup dans les actes, soit par addition ou altération de clauses, de déclarations ou de faits que ces actes avaient pour objet de recevoir et de constater.

Art. 487. (Loi du 14 août 2000) : L'incrimination spécifique de l'usage de fausses clefs.

Sont qualifiées fausses clefs:
Tous crochets, rossignols, passe-partout, clefs imitées, contrefaites ou altérées, y compris électroniques;
Les clefs qui n'ont pas été destinées par le propriétaire, locataire, aubergiste ou logeur, aux serrures, cadenas ou aux fermetures quelconques auxquelles le coupable les aura employées;
Les clefs perdues, égarées ou soustraites qui auront servi à commettre le vol.
Toutefois, l'emploi de fausses clefs ne constituera une circonstance aggravante que s'il a eu lieu pour ouvrir des objets dont l'effraction eût entraîné une aggravation de peine.

Art. 488. (Loi du 14 août 2000)

« Quiconque aura frauduleusement contrefait ou altéré des clefs, y compris électroniques sera condamné à un emprisonnement de trois mois à deux ans et à une amende de 251 euros à 2.000 euros.»

Le législateur précise que cette disposition peut s'applique au domaine informatique.

Art. 505. (Loi du 14 août 2000) : L'incrimination générale de recel

« Ceux qui auront recelé, en tout ou en partie, les choses ou les biens incorporels enlevés, détournés ou obtenus à l'aide d'un crime ou d'un délit, seront punis d'un emprisonnement de quinze jours à cinq ans et d'une amende de 251 euros à 5.000 euros.
Ils pourront, de plus, être condamnés à l'interdiction, conformément à l'article 24.
Constitue également un recel le fait de sciemment bénéficier du produit d'un crime ou d'un délit.

Art. 309. (Loi du 15 juillet 1993) L'incrimination de l'infraction de divulgation de secret d'affaire ou de fabrique

Celui qui, étant ou ayant été employé, ouvrier ou apprenti d'une entreprise commerciale, ou industrielle, soit dans un but de concurrence, soit dans l'intention de nuire à son patron, soit pour se procurer un avantage illicite, utilise ou divulgue, pendant la durée de son engagement ou endéans les deux ans qui en suivent l'expiration, les secrets d'affaires ou de fabrication dont il a eu connaissance par suite de sa situation, sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 251 euros à 12.500 euros.
Il en est de même de celui qui, ayant eu connaissance des secrets d'affaires ou de fabrication appartenant à une personne, soit par l'intermédiaire d'un employé, ouvrier ou apprenti agissant en violation des prescriptions de l'alinéa qui précède, soit par un acte contraire à la loi ou aux bonnes moeurs, utilise ces secrets ou les divulgue, soit dans un but de concurrence, soit dans l'intention de nuire à celui à qui ils appartiennent, soit pour se procurer un avantage illicite.
Est passible de la même peine celui qui, soit dans un but de concurrence, soit dans l'intention de nuire à celui à qui ils appartiennent, soit pour se procurer un avantage illicite, utilise sans en avoir le droit ou communique à

autrui des modèles, dessins ou patrons qui lui ont été confiés pour l'exécution de commandes commerciales ou industrielles.

Les tribunaux peuvent ordonner, en cas de condamnation, l'affichage ou la publication par la voie des journaux de la décision, aux frais de la personne qu'ils désignent.

Art. 460. (Loi du 19 juillet 1997) : La violation du secret des correspondances

Quiconque sera convaincu d'avoir supprimé une lettre confiée à la poste, ou de l'avoir ouverte pour en violer le secret, sera puni d'un emprisonnement de huit jours à un mois et d'une amende de 251 euros à 2.000 euros, ou d'une de ces peines seulement.

Il faut noter que ce sujet est également mentionné dans la **Constitution** du Grand Duché de Luxembourg par son Art.28 : « *Le secret des lettres est inviolable* ».

Mais attention : un employeur n'est pas la poste et cet article ne s'applique pas à l'employeur qui « censure » le courrier électronique des employés.

Art. 384. (Loi du 31 mai 1999) : La détention de représentations pornographique impliquant des mineurs.

Sera puni d'un emprisonnement d'un mois à deux ans et d'une amende de 251 euros à 12.500 euros, quiconque aura sciemment détenu des écrits, imprimés, images, photographies, films ou autres objets à caractère pornographique impliquant ou présentant des mineurs âgés de moins de 18 ans. La confiscation de ces objets sera toujours prononcée en cas de condamnation, même si la propriété n'en appartient pas au condamné ou si la condamnation est prononcée par le juge de police par l'admission de circonstances atténuantes.

Cet article mentionne « *sciemment détenu* ». Nous mesurerons l'importance de cet article lorsque nous aborderons les aspects techniques dans le chapitre quatre : la récupération des preuves dans une mémoire vive ou sur un disque. En effet, la Cour d'appel de Luxembourg⁸ a jugé que « *l'inscription automatique dans la mémoire temporaire n'est qu'une preuve de la consultation d'un site, mais non de la détention des images diffusées par le site.* »

II.3 LA RESPONSABILITE

Au Luxembourg, la responsabilité pénale des personnes morales n'existe que depuis le 4 février 2010.

⁸ 18 octobre 2006, arrêt n° 490/06 X.

II.4 CODE DU TRAVAIL, LIVRE 2, TITRE VI, ART. L. 261-1

Cet article est l'ancien Art.11 de la loi du 2 août 2002 sur la protection des données à caractère personnel.

« (1) Le traitement des données à caractère personnel à des fins de surveillance sur le lieu de « travail peut être mis en oeuvre, conformément à l'article 14 de la loi du 2 août 2002 relative « à la protection des personnes à l'égard du traitement des données à caractère personnel, par « l'employeur s'il en est le responsable. »

« Un tel traitement n'est possible que s'il est nécessaire:

« 1. pour les besoins de sécurité et de santé des travailleurs, ou

« 2. pour les besoins de protection des biens de l'entreprise, ou

« 3. pour le contrôle du processus de production portant uniquement sur les machines, ou

« 4. pour le contrôle temporaire de production ou des prestations du travailleur, lorsqu'une telle mesure est le seul moyen pour déterminer la rémunération exacte, ou

« 5. dans le cadre d'une organisation de travail selon l'horaire mobile conformément au « présent code.

« Dans les cas visés aux points 1, 4 et 5, le comité mixte d'entreprise, le cas échéant institué, a un pouvoir de « décision tel que défini à l'article L. 423-1, points 1 et 2.

« Le consentement de la personne concernée ne rend pas légitime le traitement mis en oeuvre « par l'employeur.

« (2) Sans préjudice du droit à l'information de la personne concernée, sont informés « préalablement par « l'employeur: la personne concernée, ainsi que pour les personnes tombant sous l'empire de la législation sur le « contrat de droit privé: le comité mixte ou, à défaut, la délégation du personnel ou, à défaut encore, l'Inspection « du travail et des mines; pour les personnes tombant sous l'empire d'un régime statutaire: les organismes de « représentation du personnel tels que prévus par les lois et règlements afférents. »

II.5 LA LOI MODIFIEE DU 2 AOÛT 2002 SUR LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

Au Grand Duché de Luxembourg, la loi du 2 août 2002 sur la protection des données à caractère personnel prévoit les dispositions à prendre afin de protéger ces données. Et qui dit protection, dit contrôle et surveillance.

Dans ce contexte, ce qui nous occupe plus particulièrement sera la surveillance sur le lieu de travail. C'est sur ce point que je reviendrai régulièrement⁹ car la surveillance étant un traitement intrusif, le législateur a voulu l'encadrer strictement.

Art.2. Définitions

«(p) «surveillance»: toute activité qui, opérée au moyen d'instruments techniques, consiste en l'observation, la collecte ou l'enregistrement de manière non occasionnelle des données à caractère personnel d'une ou de plusieurs personnes, relatives à des comportements, des mouvements, des communications ou à l'utilisation d'appareils électroniques et informatisés;»

Art. 10. Traitement à des fins de surveillance

(1) Le traitement à des fins de surveillance ne peut être effectué que:

(a) si la personne concernée a donné son consentement, ou

(b) aux abords ou dans tout lieu accessible ou non au public autres que les locaux d'habitation, notamment dans les parkings couverts, les gares, aéroports et les moyens de transports publics,

⁹ PIERRE-BEAUSSE, Cyril. *La protection des données personnelles*, Promoculture, Luxembourg, 2005.

pourvu que le lieu en question présente de par sa nature, sa situation, sa configuration ou sa fréquentation un risque rendant le traitement nécessaire:

«-à la sécurité des usagers ainsi qu'à la prévention des accidents;(…)

-à la protection des biens, s'il existe un risque caractérisé de vol ou de vandalisme», ou

(c) aux lieux d'accès privé dont la personne physique ou morale y domiciliée est le responsable du traitement, «ou»

«(d) si le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement.»

(2) Les personnes concernées sont informées par des moyens appropriés tels que des panneaux de signalisation, des circulaires et/ou des envois recommandés par voie postale ou électronique de la mise en oeuvre des traitements visés au paragraphe (1), lettres (b) et (c). A la demande de la personne concernée, le responsable du traitement fournit à celle-ci les informations prévues à l'article 26, paragraphe (2).

(3) Les données collectées à des fins de surveillance ne sont communiquées que:

(a) si la personne concernée a donné son consentement sauf le cas interdit par la loi, ou

(b) aux autorités publiques dans le cadre de l'article 17, paragraphe (1), ou

(c) aux autorités judiciaires compétentes pour constater ou poursuivre une infraction pénale et aux autorités judiciaires devant lesquelles un droit en justice est exercé ou défendu.

(4) Quiconque effectue un traitement en violation des dispositions du paragraphe (1) qui précède est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du paragraphe (1) du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Cette législation précise les conditions de légitimité pour implémenter un système à des fins de surveillance, c'est-à-dire le respect de l'Art.10 ainsi que du Code du Travail, Livre 2, Titre VI, Art. L. 261-1, tous deux cités ci-dessus.

Une autorisation préalable doit être demandée auprès de la CNPD¹⁰ avant toute mise en place.

Art. 26. Le droit à l'information de la personne concernée

(1) Lorsque des données sont collectées directement auprès de la personne concernée, le responsable du traitement doit fournir à la personne concernée, au plus tard lors de la collecte et quels que soient les moyens et supports employés, les informations suivantes, sauf si la personne concernée en a déjà été informée:

(a) l'identité du responsable du traitement et, le cas échéant, de son représentant;

(b) la ou les finalités déterminées du traitement auquel les données sont destinées;

(c) toute autre information supplémentaire telle que:

- les destinataires ou les catégories de destinataires auxquels les données sont susceptibles d'être communiquées;

- le fait de savoir si la réponse aux questions est obligatoire ou facultative ainsi que les

¹⁰ Commission nationale pour la protection des données (www.cnpd.lu)

conséquences éventuelles d'un défaut de réponse;

- l'existence d'un droit d'accès aux données la concernant et de rectification de ces données;

(...) abrogée par la loi du 27 juillet 2007

(Loi du 27 juillet 2007)

«dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont collectées, ces informations supplémentaires sont nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données.»

(2) Lorsque les données n'ont pas été collectées auprès de la personne concernée, le responsable du traitement doit, dès l'enregistrement des données ou, si une communication de données à un tiers est envisagée, au plus tard lors de la première communication de données, fournir à la personne concernée, sauf si elle en est déjà informée, les informations suivantes:

(a) l'identité du responsable du traitement et, le cas échéant, de son représentant;

(b) la ou les finalités déterminées du traitement auquel les données sont destinées;

(c) toute information supplémentaire telle que:

- les catégories de données concernées;

- les destinataires ou les catégories de destinataires des données auxquels les données sont susceptibles d'être communiquées;

- l'existence d'un droit d'accès aux données la concernant et de rectification de ces données;

(...) abrogée par la loi du 27 juillet 2007

(Loi du 27 juillet 2007)

«dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont collectées, ces informations supplémentaires sont nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données.»

(3) Quiconque contrevient aux dispositions du présent article est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

II.6 LA LOI DU 30 MAI 2005

Cette loi traite en outre des dispositions spécifiques de protection à l'égard du traitement des données à caractère personnel dans les communications électroniques.

II.7 AUTRES CONSIDERATIONS CONCERNANT LE RESPECT DE LA VIE PRIVEE

« Le respect de la vie privée doit aussi englober, dans une certaine mesure, le droit pour l'individu de nouer et développer des relations avec ses semblables. Il paraît, en outre, n'y avoir aucune raison de principe de considérer cette manière de comprendre la notion de « vie privée » comme excluant les activités professionnelles ou commerciales [...] dans les préoccupations de quelqu'un, on ne peut pas toujours démêler ce qui relève du domaine professionnel de ce qui en sort »¹¹

Cependant le Tribunal du Travail de Esch-sur-Alzette¹² a jugé que *« il est inadmissible que le salarié utilise, comme en l'espèce, le matériel mis à sa disposition par son employeur pour envoyer pendant son temps de travail à d'autres personnes des images à caractère particulièrement choquant [...] »*

Il faut noter que le destinataire d'un courrier en devient le propriétaire dès réception. Il a donc le droit d'en dévoiler le contenu.

Le respect de la vie privée et la surveillance

L'employeur a le droit et le devoir de veiller à la bonne marche de son entreprise et donc des outils de cette entreprise. Le courrier électronique en est un. A ce sujet, le Tribunal du Travail de Luxembourg a rendu un jugement intéressant¹³ : *« le rapport de subordination employé/employeur fait apparaître que les salariés ne peuvent guère prétendre sur leur lieu de travail à voir mener leur existence comme ils l'entendent. Il a d'ailleurs été jugé que la vie au travail est distincte de la vie privée et qu'elle relève notamment de la vie publique. »* Et de conclure : *« [...] la surveillance exercée sur le courrier électronique constitue une contrainte acceptable pour les employés. »*

Depuis ce jugement, la loi du 2 août 2002 sur la protection des données à caractère personnel a vu le jour et cette surveillance n'est plus légale si elle n'est pas explicitement autorisée par la Commission de protection des données à caractère personnel (CNPD).

Groupe de travail « Article 29 »

Ce groupe de travail a été créé en tant qu'organe consultatif par la Commission européenne. Il est composé de représentants des autorités de surveillance de chaque pays européen membre de l'UE. Il émet régulièrement des avis et donne des lignes directrices dans le domaine de la protection des données personnelles comme¹⁴ *« Si les salariés ont droit à un certain degré de la vie privée sur leur lieu de travail, ce droit ne doit pas léser celui de l'employeur de contrôler le fonctionnement de son entreprise et de se protéger contre une action des salariés susceptible de nuire à ses intérêts légitimes »*

¹¹ Cours européenne des Droits de l'Homme, affaire Niemietz c./Allemagne, 16 décembre 1992. Tiré du livre « La protection des données personnelles » (op.cit.)

¹² 21 novembre 2003, n°2518

¹³ Tribunal du Travail de Luxembourg, 30 mai 2000, Stassain / Rabobank Luxembourg.

¹⁴ Avis du 29 mai 2002.

III Chapitre deux : La preuve

« La preuve est la pierre angulaire de tout procès, la preuve informatique incontestée le Graal des avocats, experts, policiers et autres protagonistes agissant dans le domaine de la fraude informatique. »

Marie Barel¹⁵

La preuve technique est liée au domaine juridique car c'est la preuve des faits qui déclenche l'application de la disposition légale. La rencontre de l'informatique et du droit pénal est logique puisque l'informatique permet toutes sortes d'actes frauduleux qui ne sont virtuels que de nom, notamment la manipulation de comptes bancaires, le vol et la divulgation de secrets, l'usurpation d'identité, la pédophilie, le chantage.

En droit, le concept de preuve est souvent lié à celui de l'écrit, du matériel. Avec l'arrivée de l'informatique, la difficulté de la preuve vient du fait que l'objet du délit est immatériel. Il faudra donc récolter les preuves matérielles qui sont les éléments constitutifs de l'infraction pour prouver l'intention qui, elle aussi, est immatérielle. Elles devront donc être fiables afin de ne laisser aucune place à l'incertitude juridique et pour cela devront répondre à des critères stricts de recevabilité et d'admissibilité. Le support méritera donc beaucoup de soin, d'où l'importance des procédures de récolte que nous étudierons ultérieurement.

Ce chapitre traite des principes, de la charge ainsi que des moyens de la preuve. Il traite également de la fiabilité des preuves informatiques ainsi qu'un aspect tout récent –né avec Internet- de la preuve : la défense troyenne.

¹⁵ BAREL, Marie. *Fraude informatique et preuve : la quadrature du cercle ?*, [En ligne]. Adresse URL : <http://actes.sstic.org/SSTIC05/>

III.1 LES PRINCIPES DE LA PREUVE

Le Code de procédure criminelle¹⁶ énonce les principes¹⁷ de la preuve en matière pénale.

La liberté de la preuve

*1° L'article 154 qui spécifie quelques modes de preuve, n'est pas limitatif; en matière correctionnelle aussi bien qu'en matière criminelle, **la preuve n'est assujettie à aucune forme spéciale et systématique**; les juges du fond peuvent librement former leur conviction, en faisant état de tout élément de l'instruction qui a pu être **l'objet du débat contradictoire**; [...]*

La publicité de la preuve

*2° En matière répressive, le juge doit prendre pour base de sa décision son intime conviction qu'il peut puiser dans tous **les éléments des débats ayant eu lieu en audience publique**; il apprécie souverainement tous les faits de la cause [...].*

*4° Les juridictions répressives ne sont pas tenues de former leur conviction sur les seuls moyens de preuve énoncés dans les articles 154 et 189 du Code d'instruction criminelle. Elles peuvent **s'appuyer sur tous autres moyens, pourvu qu'ils soient soumis au débat**, et la loi ne leur interdit pas de fonder leur conviction sur de simples présomptions, dès lors que les faits qui en forment la base ont été produits à l'audience [...].*

Le doute

*3° S'il est généralement admis que le juge pénal fonde sa décision sur l'intime conviction, il faut cependant que cette conviction résulte de **moyens de preuve légalement admis et administrés dans les formes**; en d'autres termes la conviction du juge doit être l'effet d'une preuve, conclusion d'un travail préliminaire de réflexion et de raisonnement, ne laissant plus de doute dans l'esprit d'une personne raisonnable.*

***La vraisemblance**, même très grande, surtout lorsqu'elle ne résulte que d'une preuve circonstancielle, **ne saurait à elle seule former la conviction** du juge pénal, puisque cette preuve est par nature indirecte, complexe et fragmentaire, rendant peu sûres les inférences tirées du concours des indices recueillis contre le prévenu.*

La vraisemblance du fait imputé au prévenu peut finalement n'être qu'un concours de circonstances fondé sur une preuve par indices non pas univoques, mais équivoques. Une telle preuve est insuffisante pour entraîner la conviction du juge [...].

Cependant, si l'on considère la « *Convention de sauvegarde des droits de l'homme et des libertés fondamentales* »¹⁸, ce droit comporte des exceptions, notamment dans l'intérêt de l'administration de la justice.

¹⁶ Livre II, Titre 1^{er}, Le régime des preuves

¹⁷ Voir également Annexe 1.

¹⁸ « *Convention de sauvegarde des droits de l'homme et des libertés fondamentales* », ouverte à la signature le 4 novembre 1950, ratifiée par le Luxembourg le 3 septembre 1953.

La loyauté de la preuve

Une preuve est loyale lorsqu'elle a été obtenue d'une infraction sans qu'il y ait eu provocation à cette infraction.

L'arrêt de la Cour d'Appel de Luxembourg, cinquième chambre, siégeant en matière correctionnelle et après renvoi suite à l'arrêt de la Cour de cassation du 22 novembre 2007 dans l'affaire dite « *Wagner* »¹⁹ est intéressant car il refuse de reconnaître comme preuve l'enregistrement par des caméras non autorisées par la CNPD.

La loyauté de la preuve vient donc limiter la liberté de la preuve en matière pénale : une preuve détenue par des moyens déloyaux, notamment illégaux, est irrecevable !

III.2 LA CHARGE DE LA PREUVE

La charge de la preuve en incombe à celui qui veut faire établir un fait ou un droit. Le doute profitera toujours à l'accusé. Dans de rares cas, des présomptions peuvent dispenser celui qui doit prouver un fait impossible ou difficile à prouver.

« *Lorsqu'un prévenu allègue une circonstance qui exclut sa culpabilité et que cette allégation n'est pas dénuée de tout élément permettant de lui accorder crédit, il incombe au ministère public d'établir l'inexactitude de cette allégation.* »²⁰

III.3 AUTRES MOYENS DE PREUVE

La preuve testimoniale

Le Code d'instruction criminelle (CIC) contient de longues dispositions relatives à la preuve testimoniale dont une partie dédiée à l'expertise. L'Art.158 de ce CIC est relatif au régime des preuves, notamment celui du témoignage de l'expert. Ce témoignage de l'expert sera considéré dans la dernière partie de ce travail.

La preuve négative

En droit, la preuve négative « *probatio diabolica* » se rapporte à un fait positif comme par exemple l'existence d'un système de sécurité.

Il s'agit ici de faire la preuve de l'absence de négligence ou de dysfonctionnement du système qui a fait l'objet d'une attaque. En effet, dans le cas où le propriétaire du système aurait laissé « la porte ouverte », l'accusé potentiel pourrait arguer du fait qu'il n'a franchi aucune barrière lui interdisant l'accès. Un argument de plus en faveur d'une politique de sécurité forte.

¹⁹ Arrêt n°106/08 V. du 26 février 2008. Voir extraits en Annexe 1.

²⁰ Cassation. 27 octobre 1977, 24, 7.

III.4 L'ÉLÉMENT HUMAIN ET LA DÉFENSE TROYENNE

Il faut encore prouver l'élément humain, encore appelé psychologique ou moral. Cet élément moral est intentionnel, c'est-à-dire que l'auteur de l'infraction a agi « *sans droit et en connaissance de cause* »²¹. Prouver l'intention est devenu difficile car avec l'évolution de l'informatique et des réseaux est apparue une nouvelle forme de défense : la défense troyenne.

L'accusé argumente que la preuve trouvée dans son ordinateur est en fait due à la présence d'un cheval de Troie, d'où le qualificatif « troyenne ». Cette défense constitue un obstacle de taille lorsqu'il s'agit de prouver que l'accusé est en fait responsable de la preuve trouvée sur son ordinateur. En effet, ce mode de défense jette le doute dans les esprits car, comme le dit Mark Rasch²² : « *this defence is all the more frightening because it could be true. If you were a hacker, would you want to store your contraband files on your own machine, or, like the cuckoo, would you keep your eggs in another bird's nest?* »

Cette forme de défense est souvent citée dans les relations de cas de cours, au Royaume Uni notamment, et inquiète : "*The acquittal of a teenager accused of carrying out a high-profile hack attack has cast doubts over future computer crime prosecutions, say experts.*"²³

Il faudra donc prouver le caractère intentionnel²⁴.

Mais heureusement ces techniques ne sont pas tout ce dont nous disposons et d'autres éléments peuvent démonter cette défense troyenne : si l'individu soupçonné d'être l'auteur de l'infraction refuse de collaborer, s'il commet une action anti-forensique ou encore s'il franchit plusieurs défenses techniques dans le système attaqué, toutes ces actions démontreront qu'il y a réellement intention frauduleuse comme précisé dans l'Art 509 du Code Pénal vu précédemment.

Il est à noter que ce genre de défense est également utilisé dans le cas d'une attaque par rebond, cas dans lequel un attaquant prend possession d'un système et s'en sert comme base pour ses attaques ultérieures.

III.5 FIABILITE DES PREUVES INFORMATIQUES²⁵

Une preuve n'a de sens que si les données sont intègres. Il faut faire une différence entre la preuve de l'intégrité et l'intégrité de la preuve. Le premier aspect implique que tous les moyens sont mis en œuvre en amont pour préserver l'intégrité de ce qui se passe en aval, notamment la logique et l'exactitude des traitements ce qui permet une journalisation fiable des événements. Les mécanismes de preuve devraient être omniprésents durant toute la chaîne informatique, de la conception à l'exploitation des programmes et systèmes.

²¹ Marie Barel (op.cit.) citant l'arrêt de la Cour d'Appel de Paris du 5 avril 1994.

²² RASCH, Mark. *The Giant Wooden Horse Did It!*, [En ligne]. Adresse URL: www.SecurityFocus.com

²³ « Questions cloud cyber crime cases », BBC News UK Edition, 17 octobre 2003

²⁴ Pour le technicien averti : www.sciencedirect.com recherche sur : Trojan defence, Haagman.

²⁵ Paragraphe inspiré par le cours « *Le contexte sectoriel* » de David Hagen dans le cursus du Master MSSI.

L'intégrité de la preuve signifie qu'elle n'a pas été altérée depuis sa récolte ce qui implique qu'elle doit être sauvegardée correctement. Déjà en 1998, dans un litige qui l'opposait à un employé, la société IBM ne put pas utiliser les preuves qu'elle avait récoltées car le disque qui les contenait n'avait pas été conservé sous séquestre et donc était susceptible d'avoir été altéré²⁶.

Ces deux aspects (intégrité et conservation) sont importants car on parle ici de *fiabilité*. Or l'intégrité d'une donnée signifie que toute modification de cette donnée est volontaire et résulte de l'exécution d'un processus sous contrôle. Cela ne signifie pas qu'elle soit fiable (selon le bien connu « *Garbage in, garbage out* »). Il faut donc garantir la preuve en amont, au niveau des traitements, en mettant en place les mécanismes qui garantiront l'inaltérabilité des programmes par l'application d'un principe de quatre yeux, d'outils de gestion des versions et de mise en production.

Nous pouvons donc avancer que la preuve est garantie par la vérification des informations avant et après traitement, sur base d'une journalisation²⁷. Le terme informatique approprié est « *trace d'audit, inaltérable et exhaustive* ».

III.6 UNE PREUVE IRREPROCHABLE

L'appréciation libre du juge va peser sur la nature même de la preuve. Il faut donc, et cela ne sera jamais suffisamment répété, que les preuves présentées soient irréprochables :

- Précautions techniques pour la capture des données : multiplication des sources (recoupements, sauvegarde, reconstruction des séquences du délit) ;
- Précautions techniques pour la conservation des données : conservation sur un tiers de confiance;
- Preuve récoltée par des moyens légaux ;
- Mise en évidence d'actions anti-forensiques (effacement) car « ce que l'on cache vaut bien ce que l'on trouve »²⁸
- Police versus privé : le particulier n'a pas, au contraire de la police, à respecter le Code de procédure pénale. Cette considération est évidemment limitée par le principe de loyauté de la preuve.

²⁶ Conseil des Prud'hommes de Nanterre (FR), 16 novembre 2000.

²⁷ Voir Chapitre 4, IV.3.1.1

²⁸ ROGER, Laurent. *Antiforensic*, [En ligne]. Adresse URL : http://actes.sstic.org/SSTIC05/Anti_forensic/

IV Chapitre trois: la criminalité informatique dans l'entreprise.

“Internal security breaches have overtaken external IT attacks as the biggest threat to financial institutions as hackers switch their focus from technology to people”.

Deloitte'2005 Global Security Survey

Protéger les informations sensibles contre des manipulations non autorisées et la divulgation par les personnes y ayant légalement accès est devenu une préoccupation majeure de toutes les entreprises. Alors que jusque récemment encore, l'entreprise mettait l'accent sur la protection contre les agressions venant de l'extérieur en installant des firewalls et autres outils de détection, aujourd'hui les agressions viennent de l'intérieur. Les employés, les dirigeants, les contractants et toutes les autres personnes prenant part à la vie de l'entreprise sont une menace importante vu leur connaissance et leurs accès autorisés aux systèmes d'information. Les menaces internes sont plus difficiles à détecter que les menaces externes. En effet, il est plus difficile d'identifier l'individu bénéficiant d'un accès autorisé que de bloquer l'accès (par hypothèse non autorisé) d'un attaquant externe. Bien souvent aussi, le manque de précision dans les procédures fait qu'il est difficile de savoir où se situe exactement la limite à ne pas franchir.

Le fait que les entreprises ouvrent leurs réseaux à un plus grand nombre de personnes, employés classiques mais aussi employés à distance, partenaires, clients, consultants, ... fait que la définition et les limites de la menace interne se sont élargies. En effet, ces nouveaux intervenants sont considérés « de confiance » et ont donc accès à l'information de l'entreprise. L'entreprise et son système d'information sont donc proportionnellement plus exposés.

Il faut insister sur le fait que détecter et manager la criminalité informatique des employés est du ressort de l'entreprise. En effet, trop souvent encore, on continue à croire que combattre les menaces internes est le même combat que combattre les menaces externes. Ce serait oublier que ces menaces peuvent également résulter de l'incompétence, de l'ignorance et de la négligence. S'il y a bien quelques rapports officiels, il faut bien dire que les chiffres avancés dans ces rapports ne sont probablement que le sommet visible de l'iceberg. Ces chiffres partiels ne peuvent pas en eux-mêmes rendre compte de la réalité d'un phénomène dont il faut plutôt étudier les motivations.

IV.1 L'ANALYSE SOCIOLOGIQUE

La nature même de la fraude informatique est complexe. Beaucoup de chercheurs²⁹ considèrent que l'employé commettant une fraude informatique est motivé par l'avidité, l'égoïsme et l'individualisme qui sont inhérents aux valeurs de la société capitaliste. Tout cela associé aux émotions et besoins humains en fait la première motivation de criminalité informatique.

Il n'est cependant pas facile de lier la criminalité informatique à des pathologies individuelles et, en conséquence, quasiment impossible d'établir un portrait type. Mais il ne faut pas tomber dans l'excès contraire en considérant que les faits de criminalité informatique ne sont dus qu'à des cas isolés.

Il faut donc analyser les relations {individu - organisation - facteurs sociologiques}, ce qui implique une bonne connaissance des pratiques de l'entreprise elle-même ainsi que des valeurs culturelles qui généralement encouragent ou découragent la fraude car la culture est prédominante chez l'homme.

Selon H.Croall³⁰ « *le but principal de punir les criminels est la dissuasion* ». Il apparaît que les politiques de sécurité, les programmes d'information, les logiciels de sécurité préventive et d'autres sont des forces de dissuasion car elles montrent clairement aux attaquants potentiels que le risque de se faire prendre est grand et la punition sévère. L'aspect dissuasif de cette punition pourrait être augmenté si nous pouvions utiliser des cas jugés par les tribunaux comme exemples. Malheureusement, spécialement au Grand Duché, il y a peu de matière car les entreprises hésitent encore souvent à porter plainte pour les raisons énoncées ci-dessus mais également parce qu'il n'apparaît pas clairement aux yeux du public que la justice possède les armes pour juger efficacement ces délits.

Par contre, le manque de mesures de sécurité crée un environnement dans lequel les employés ne se sentent en aucune façon responsables des conséquences de leurs actions et pourraient avec justesse les rejeter sur d'autres acteurs tels que les collègues. Une telle situation contribue certainement à la fraude.

Cela démontre que les dirigeants ont une responsabilité énorme dans la sécurité de leur entreprise puisque de par leurs décisions, ils influencent directement la structure de cette entreprise et donc l'occurrence de la fraude.

²⁹ Les références sociologiques et psychologiques de ce chapitre sont tirées d'un texte de Shalini Kesar, Université de Liverpool, et empruntées à divers chercheurs: **Hazel Croall**, Senior Lecturer and Head of Division of Sociology at the University of Strathclyde, dans son livre « *White Collar and Corporate Crime* », Open University Press, Milton Keynes, UK (1992) ; **Dr. Eugene Schultz**, Principal Engineer with Lawrence Berkeley National Laboratory. Ph.D., CISSP, CISM; **Kesar and Rogerson**, "Developing Ethical Practices to Minimize Computer Misuse", *Social Science Computer Review*. 1998;

³⁰ *ibid*

IV.2 LES RAPPORTS OFFICIELS

Différents rapports officiels récents donnent raison à ces sociologues.

La plupart de ces rapports sont anglais et américains. Mais il est vrai que la sécurité de l'information est ancrée dans la culture anglo-saxonne depuis plus longtemps que chez nous. Mais ne dit-on pas que ce qui se passe aux Etats-Unis ne tarde pas à arriver chez nous ?

Le « *Deloitte's 2005 Global Security Survey* » est très clair quant aux chiffres de la criminalité interne: “[...] the extend of internal breaches more than doubled with 35% of respondents encountering attacks from the inside within the last twelve months, compared to 14% the year before” .

Le « *Audit Commission Report* »³¹ met en exergue que le manque de mesures de sécurité aggravé par un audit interne de mauvaise qualité est le fondement des conditions qui favorisent la criminalité informatique.

Le très connu et considéré « *CSI / FBI Survey 2007* »³² met en avant “*Insider abuse of network access or e-mail (such as trafficking in pornography or pirated software) edged out virus incidents as the most prevalent security problem, with 59 and 52 percent of respondents reporting each respectively.*”

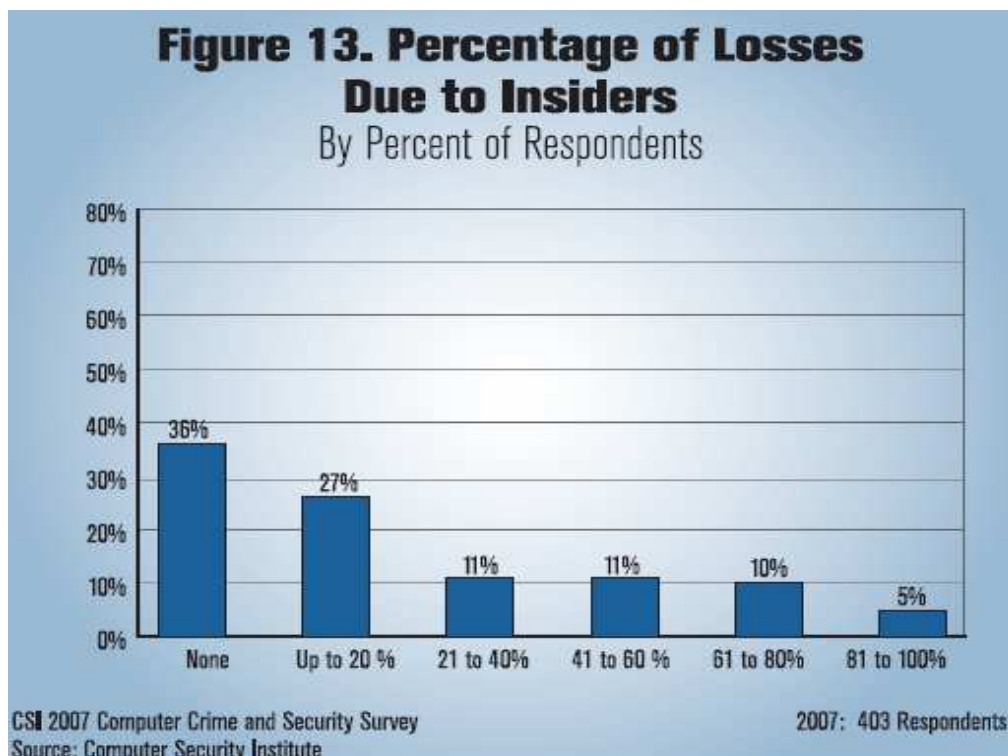


Figure 1 Pertes des entreprises dues aux attaques internes (Source : CSI 2007)

³¹Audit Commission 2001, 2005 (<http://www.audit-commission.gov.uk/> :independent body responsible for ensuring that public money is spent economically, efficiently and effectively)

³²“CSI Computer Crime and Security Survey”, 2007, Robert Richardson, director of Computer Security Institute in cooperation with Federal Bureau of Investigations.

Probablement la plus célèbre³³, l'étude "*Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector*" révèle que l'attaquant interne typique est un employé –homme (58%) ou femme (42%)- étant en service depuis plusieurs années, n'ayant pas le profil d'un employé à problèmes, n'occupant pas une position technique mais étant autorisé à accéder aux informations qu'il attaque pendant les heures de travail. On est loin ici du profil traditionnel du pirate du net...

Les autres résultats marquant de cette enquête nous montrent que :

- ⊗ la plupart des incidents (78%) ne requièrent pas de techniques sophistiquées mais simplement l'emploi des fonctions auxquelles l'attaquant est habilité et autorisé ;
- ⊗ les auteurs ont planifiés leurs actions
- ⊗ la motivation première est le gain financier, souvent en complicité avec l'extérieur, crime organisé ou concurrence. Loin derrière viennent la revanche, l'insatisfaction et le désir de respect ;
- ⊗ il n'y a pas de profil type de l'attaquant interne ;
- ⊗ les incidents furent détectés par des méthodes et personnes différentes, pas seulement par les préposés à la sécurité.

Il ressort de tout ceci que le moyen le plus approprié de combattre ces menaces internes est d'avoir une stratégie de développement de « *techniques de sécurité* », faites de politiques, procédures et contrôles. Car une chose est certaine : au plus les processus business seront automatisés, au plus il faudra être vigilant. La perte en fin d'année 2007 de cinq milliards d'euros par la Société Générale en est peut-être le meilleur exemple.

IV.3 AU GRAND DUCHE DE LUXEMBOURG

Malheureusement aucun de ces rapports ne concerne le Grand Duché. Pourquoi ? Plusieurs facteurs peuvent expliquer cette situation : la petite taille du pays, la culture du secret, la peur d'une mauvaise image, ... Je ne me prononcerai pas sur ce sujet mais il convient de signaler que depuis 2007 la CSSF³⁴ demande aux professionnels du secteur financier de lui adresser un rapport reprenant les incidents de sécurité dont ils ont été victimes.

Cette situation est mise en exergue par Jean-Philippe Humbert dans sa thèse de doctorat « *Les mondes de la cyberdélinquance et images sociales du pirate* »³⁵. Même si cette étude ne vise pas spécifiquement la criminalité en entreprise, il rapporte que l'absence de mesure fédérée nationale est reconnue comme un problème par ses divers interlocuteurs. Interlocuteurs qui précisent pourtant que « *Relever ou fédérer les incidents, pour les distribuer vers tous ensuite, semble être une idée fédératrice ; mais cela devra demeurer anonyme, sur le même principe*

³³ "Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector", US Secret Service National Threat Assessment Center and the CERT Coordination Center of the Carnegie Mellon University's Software Engineering Institute in 2005.

³⁴ Commission de Surveillance du Secteur Financier

³⁵ HUMBERT, Jean-Philippe. « *Les mondes de la cyberdélinquance et images sociales du pirate informatique* », Thèse pour le doctorat en sciences de l'information et de la communication, Université Paul Verlaine-Metz, 26 octobre 2007, [En ligne]. Adresse URL : <http://www.cases.public.lu/fr/publications/>

de l'enquête du CSI/FBI, par exemple. Des entités comme les Chambres de Commerce et des Métiers peuvent procéder à l'anonymisation [...] »

A quand donc des chiffres qui ne pourraient qu'être utiles dans cette lutte ?

IV.4 L'INGENIERIE SOCIALE OU L'IMPORTANCE DU FACTEUR HUMAIN

Mieux connu sous le nom anglais de « *social engineering* », cet aspect accentue encore la menace interne par le fait que les pirates traditionnels ont changé de cible : de la cible technologique, ils s'attaquent maintenant à la cible humaine. Cette technique consiste à entrer en contact avec quelqu'un de façon à lui extorquer un maximum d'informations qui serviront plus tard d'outils pour attaquer le système d'information. Et cette activité ne s'exerce pas seulement via les technologies informatiques : elle se pratique dans des endroits publics devant un bon verre, entre collègues, par téléphone ou même en pénétrant une entreprise après avoir usurpé une identité d'intervenant externe par exemple.

Probablement le plus connu des spécialistes de cette discipline fut Kevin Mitnick qui, dans son livre « *L'art de la supercherie* »³⁶ a popularisé cette pratique. Il démontre que l'être humain doit être au centre de la politique de protection des données : aucun élément technique ne sera jamais assez efficace pour arrêter des individus déterminés à pénétrer un réseau ou à obtenir une information confidentielle. L'élément humain est à la fois la clé et le principal point faible des systèmes de sécurité : un personnel peu ou mal formé, ou qui ne respecte pas les consignes, constituera une cible privilégiée pour les hackers.

Jean-Philippe Humbert le décrit bien³⁷ : « *Toute externe qu'elle soit, la menace doit surtout aussi être perçue en interne ; pour ce faire, une troisième voie associée à la gestion des risques de sécurité, devient fondamentale, à savoir la sensibilisation aux menaces adaptée à la politique sécurité de l'organisation. En effet, la prise en compte du phénomène en interne est majeure si l'on veut éviter de créer des points d'accroches aux agents menaçants. Cette conscience doit être parallèle à celle développée lors de l'analyse de risque de sécurité vis-à-vis des bases de connaissance des menaces. Parallèlement au « sondage » technique vu supra, et en ligne avec la politique de sécurité, le RSSI se doit de sonder également les représentations mentales des employés quant aux menaces. Ainsi, il peut percevoir les absences de connaissance flagrante et dangereuse pouvant nuire à l'organisation, car traduisant notamment une incompréhension de la politique de sécurité en place. Pour ce faire, des questionnaires adaptés peuvent être proposés, aux fins de mesure, reprenant les images associées aux menaces et véhiculées par les médias, les experts sécurité et les pirates informatiques. Ces types de questionnaires (par exemple : <http://jph.cases-cc.org>) peuvent être déroulés durant une séance de sensibilisation à la sécurité des systèmes d'information, et en fonction des réponses, créer le débat, apporter des réponses concrètes et objectives permettant de faire le lien avec la politique de sécurité en cours et sa justification. Le RSSI pourra aussi bénéficier utilement de l'aide didactique fournie par la structure CASES (<http://www.cases.lu>)»*

³⁶ MITNICK, Kevin. *L'art de la supercherie* », CampusPress, Paris, 2005. Kevin Mitnick fut un hacker activement recherché par le FBI et condamné à 5 ans de prison pour s'être introduit dans différents systèmes informatiques dont ceux de Fujitsu, Siemens, Motorola et Sun Microsystems.

³⁷ *ibid*

Une autre manière peut également être d'étudier les comportements afin d'améliorer le traitement préventif de la sécurité. C'est ce que le concept du *honeypot* peut nous aider à réaliser.

IV.5 LE HONEYPOT COMME INSTRUMENT DE MESURE

Un adage bien connu des militaires est qu'il faut connaître son ennemi afin de pouvoir anticiper ses actions et pouvoir se défendre. Il en va de même dans le domaine de l'informatique à la différence que l'ennemi n'est pas connu et que ses moyens d'attaque augmentent chaque jour. Il faut donc être continuellement à l'affût de ces nouvelles techniques. C'est ici que le pot de miel intervient.

Mieux connu sous le nom anglais de *honeypot*, cette technique est d'abord utilisée pour attirer les pirates du net³⁸ : un « faux » site Internet est mis en place avec un contenu suffisamment attirant (mais sans valeur) pour soulever la curiosité des pirates potentiels. En fait, un leurre. Les pirates vont l'attaquer en utilisant toutes les armes dont ils disposent. Comme ce site Internet n'est destiné à aucun utilisateur et qu'aucune activité n'y est prévue, tout accès quel qu'il soit sera considéré comme anormal. Les activités seront enregistrées de manière passive puis analysées par la suite ce qui permettra d'étudier la façon de procéder des attaquants et d'en tirer des leçons utiles afin de mettre au point des techniques de sécurité³⁹. C'est le but premier d'un *honeypot*. Mais il est également possible de s'en servir afin d'identifier l'attaquant pour le poursuivre en justice. Cependant dans ce cas, on peut légitimement se poser des questions quant aux aspects éthique et juridique d'un tel procédé. Et c'est sans parler de la responsabilité du « propriétaire » du site hacké en cas d'attaque par rebond ayant pour base ce site.

Mais cette technique de *honeypot* peut également être utilisée pour étudier le comportement des utilisateurs au sein d'une organisation. C'est sur cet aspect que je vais m'attarder un peu plus longuement. Plusieurs expériences ont été faites dont certaines dans le contexte des cours du Master MSSI de l'Université de Luxembourg avec des résultats intéressants. Voici comment s'est déroulée la mienne⁴⁰.

Le concept repose sur un programme interactif déployé, à leur insu, sur le poste de travail des utilisateurs. Cliquer sur ce nouvel icône du bureau - suffisamment visible pour qu'un utilisateur la remarque - donnait accès à un écran intitulé « Ressources Humaines – Calcul des salaires ». Une fois sur cet écran, l'utilisateur avait la possibilité de cliquer sur « Entrer » ou « Sortir ». Le fait de choisir d'entrer dans le programme génèrait un message avertissant l'utilisateur que cet accès était réservé aux ressources humaines ; mais la possibilité de continuer existait. Si le choix d'entrer était fait, apparaissait alors un écran intitulé « Salaires employés » avec encore la possibilité de continuer ou de sortir. Le choix de continuer génèrait alors un message d'alerte virale. Toutes les transactions étaient journalisées de façon anonyme.

Le scénario de ce programme permet de vérifier des comportements qui présentent graduellement un risque pour les actifs d'une entité tels les comportements ludiques,

³⁸ La plus remarquable de ces initiatives est sans aucun doute [www.honeynet.org](http://www honeynet.org), projet international.

³⁹ Pour le technicien averti : « Know your enemy : a forensics analysis », [www.honeynet.org/papers/forensics](http://www honeynet.org/papers/forensics).

⁴⁰ Travail présenté par Alex Rosevègue, Philippe Stassin et Philippe Jeanbaptiste

négligents ou cupides. L'étude des comportements repose sur les fondements de la psychologie sociale en matière d'éthique et de responsabilité professionnelle. Le choix du contenu de ce *honeypot* repose sur l'hypothèse que ces informations représentent de la valeur, d'un point de vue culturel, aux yeux des collaborateurs.

Ce *honeypot* est donc un système d'information volontairement vulnérable destiné à jauger le comportement des collaborateurs qui peut être potentiellement négligeant ou malveillant. La philosophie de ce système est de connaître les utilisateurs, pour les satisfaire le mieux possible et les sensibiliser efficacement.

Les buts de ce *honeypot* sont multiples :

- Disposer d'un outil marketing à l'usage des responsables de la sécurité permettant de mesurer le niveau d'efficacité de la politique de sécurité de l'entreprise en mesurant la faculté des utilisateurs à repérer des changements sur leur ordinateur et en établissant le degré de non respect des règles par les utilisateurs et, corollairement, déduire le niveau de confiance vis-à-vis des utilisateurs.
- Fournir des mesures quantifiables pour permettre à ces responsables d'affiner la politique de sécurité en collaboration avec la direction de l'entreprise.
- Permettre de cibler une campagne de sensibilisation des collaborateurs.

Les enseignements que nous pourrions tirer de l'exploitation d'un tel dispositif sont multiples :

- Le fait de découvrir l'icône intrus est déjà une indication quant à la connaissance qu'ont les employés de leur environnement de travail.
- L'utilisateur a le choix : il peut lancer le programme ou simplement appeler le helpdesk pour prévenir de l'apparition d'un nouveau programme inconnu.
- Le nombre d'utilisateurs ayant ouvert l'application donne une idée de la curiosité qui les motive. En supposant que ces utilisateurs soient sensibilisés aux problèmes de sécurité, on peut conclure à un début de négligence ou de malveillance.
- L'utilisateur est dans un état « *j'y accède, donc j'ai le droit* » qui est directement lié à son éthique personnelle. S'il continue, il choisit délibérément de s'installer dans un programme qui, de toute évidence, ne lui est pas destiné. Il se trouve dans la situation où il peut accéder à des données ayant de la valeur sans que son nom soit associé à la transgression puisqu'il n'y a pas d'authentification. Cela peut mesurer son appétence aux titres évocateurs des menus.
- La réaction à l'apparition de la menace virale est d'importance : l'utilisateur se trouve face au fait de devoir prendre ses responsabilités alors qu'il a transgressé des règles.

Au vu des enseignements tirés de ce concept, il s'avère que ce *honeypot* peut être utile dans la définition et la mise en place d'une politique de sécurité. Cependant ce système pose un problème éthique et légal. En effet, s'agit-il de contrôle ou de surveillance ? Qu'en est-il du respect de la loi sur la protection des données à caractère personnel ainsi que du Code du travail concernant la surveillance des salariés sur le lieu de travail ? Peut-on assimiler un tel système à de la provocation⁴¹ ? Peut-on considérer que le fait de mettre « du miel dans le

⁴¹ Cette question est posée par Marie Barel (Op.cit.). D'après Cyril Pierre-Beausse (Op.cit.), au Grand Duché de Luxembourg, mettre en place un site n'est pas une incitation au délit et son attaque n'est certainement pas couverte par une excuse pénale ou autre.

pot »⁴² constitue à la fois une forme de consentement implicite de l'employeur en même temps qu'une négligence coupable ?

L'implémentation d'un tel système requiert la plus grande prudence quant au respect de la législation luxembourgeoise, tant sur le plan de la protection des données à caractère privé que sur le plan de la surveillance sur le lieu de travail. Aucun des critères contenu dans l'article L.261-1 du Code du travail ne permet en l'espèce de justifier l'implémentation du honeypot tel que nous l'avons conçu.

Il est donc primordial de veiller à ce qu'aucune donnée nominative telle que l'identifiant de l'utilisateur ne soit enregistrée dans les logs de l'application. On veillera également à n'enregistrer aucune donnée telle qu'une adresse IP ou l'identifiant du poste de travail qui permettrait de retracer son origine ou son auteur. De plus, toutes les précautions doivent être prises, notamment dans la documentation de la finalité du projet, afin de ne pas assimiler l'initiative du honeypot à de la surveillance sur le lieu de travail. Il est donc important de justifier la finalité du projet par la mise en œuvre d'un indicateur purement statistique permettant de mesurer l'efficacité des campagnes de sensibilisations des employés aux problématiques de la sécurité et non de surveiller la disposition des employés à transgresser les règles.

Bien qu'aucune donnée nominative ne soit enregistrée par l'application, un risque pourrait subsister de par la notification de la détection d'un virus. En effet, si l'utilisateur, en réaction à cette notification, notifie à son tour le Helpdesk, son appel et ses coordonnées nominatives sont enregistrés. Afin d'éviter de pouvoir établir un lien entre l'appel au Helpdesk, il faut associer ce Helpdesk au projet et lui demander de ne pas enregistrer les appels, seulement de les compter.

Le distinguo entre un faux et un véritable message d'alerte est permis par la description du virus fourni lors de la notification de l'alerte à l'utilisateur. En cas de doute, le Helpdesk vérifierait sur ses consoles d'administration si un problème réel a été détecté par le système de gestion de l'anti-virus de l'entreprise.

Autorisation préalable de la CNPD⁴³

Si la solution du honeypot avait rendu possible la collecte de données nominatives ou de toute autre information permettant d'effectuer le rapprochement entre le contenu des logs et de l'employé à l'origine des actions enregistrées, il se serait agi d'une surveillance sur le lieu de travail et l'article 11 de la loi modifiée du 2 août 2002 eut été applicable. Or, aucune base légale ne permet de justifier cette surveillance et il est donc impossible d'obtenir l'autorisation préalable de la CNPD. Cela serait impossible sans le consentement des personnes concernées et ce consentement ruinerait le projet.

Dans pareil projet, **il est donc bien indispensable**, pour éviter d'entrer dans le champ d'application de la loi, **de ne traiter aucune donnée à caractère personnel**. C'est uniquement dans ce contexte **d'anonymat total** que l'obtention de l'autorisation préalable de la CNPD n'est pas requise.

⁴² BAREL, Marie. *Honeypot : un pot-pourri...juridique*, [En ligne]. Adresse URL: <http://actes.sstic.org/SSTIC04/>

⁴³ Cet aspect sera traité ultérieurement.

V Chapitre quatre: Les fraudes

« Fraude : employer des moyens trompeurs et exploiter la confiance acquise pour obtenir illégalement un avantage personnel ou au bénéfice de tiers »

« La fraude informatique n'a pas vraiment d'essence propre; cette appellation recouvre en fait toute fraude accomplie à l'aide d'un ordinateur plutôt qu'avec les outils traditionnels que sont le papier et le stylo.»

Ernst & Young Belgique⁴⁴

Ce chapitre n'a pas la prétention de recenser toutes les attaques dont une entreprise pourrait un jour être la cible : en effet, l'imagination des cybers délinquants n'a d'égale que l'évolution étourdissante de la technologie.

Mais, comme déjà précisé, les fraudes sont tout sauf virtuelles et les moyens informatiques ne sont que des outils pour les commettre. Parmi les agissements frauduleux, on retrouve pêle-mêle :

- La compromission et le vol d'information ;
- L'utilisation de l'ordinateur de l'entreprise comme base d'attaque vers l'extérieur ;
- L'atteinte à la disponibilité des services ;
- L'usurpation d'identité ;
- Pédo pornographie ;
- Non respect de la propriété intellectuelle ;
- L'espionnage ;
- Les logiciels malveillants ;
- Atteinte à la vie privée
- ...

En informatique comme dans d'autres domaines, les délits laissent des traces. C'est l'aspect technologique de ces traces que ce chapitre considère.

⁴⁴ www.ey.be

V.1 LE DENOMINATEUR COMMUN : LES TRACES D'UTILISATION

Chaque intervention –humaine ou technique- sur un système d'information laisse des traces. C'est inhérent à l'informatique. La sécurité d'un système d'information s'appuie d'ailleurs sur le contrôle de ces traces : contrôle opérationnel du système, détection d'anomalies, vérification de l'application des politiques de sécurité. A ce stade nous ne parlons pas encore de fraude.

Si l'on considère maintenant ce caractère frauduleux, les traces pourront servir de preuves pour autant qu'elles aient été recueillies suivant une procédure légale. Nous y reviendrons plus tard.

A noter que le concept de traces ne contient pas les produits des interventions : un e-mail par exemple est le produit d'une intervention qui a laissé des traces sur le serveur de messagerie.

Quelles sont ces traces ?

En général

- L'identification de l'utilisateur : l'identification la plus fréquente est certainement le « *userID* » ; mais d'autres traces permettent d'identifier l'utilisateur indirectement comme, par exemple, l'adresse IP de son ordinateur.
- L'adresse IP, l'adresse MAC : expérience à faire : se connecter sur www.celog.fr/infocensique.php .
- L'heure et la date : ces informations sont fonctions du temps réel affiché par l'horloge système, du système d'exploitation lui-même, des applications accédant à ces fichiers, des fuseaux horaires. Pour l'œil humain, la date et l'heure apparaissent de même façon lisible. Par contre, la façon dont sont interprétées ces données est différente d'un système d'exploitation à l'autre. Par exemple, sur un système Unix la date et l'heure sont une valeur numérique de 4 bytes représentant le nombre de seconde depuis le 1^{er} janvier 1970 et chez Windows il s'agit d'une valeur numérique de 8 bytes représentant le nombre de nanosecondes depuis le 1er janvier 1601! Les fuseaux horaires (*time zones*) ainsi que l'heure d'été/hivers doivent également être pris en considération. Certains systèmes convertissent les valeurs en temps GMT, d'autres laissent ces valeurs en temps local.⁴⁵
- Le résultat de l'intervention : succès ou échec
- Le nombre de connexions
- Les différentes commandes passées
- Les volumes manipulés

Spécifique à la messagerie :

- L'adresse expéditeur / destinataire
- Un certificat le cas échéant
- Le sujet du message s'il contient des caractères non standards

⁴⁵ Voir l'excellent papier de K.Stone et M.Roter à ce sujet : www.guidancesoftware.com/downloads/

Spécifique serveur Web

- Les pages consultées
- Les ports (source et destination) et le protocole utilisés
- Le type de requête

Spécifique équipement de sécurité

- Les ports (source et destination) et le protocole utilisés
- Le nombre de paquets, d'octets

Spécifique aux applications :

Chaque application peut avoir un système d'enregistrement des traces qui lui est propre.

Il est donc clair que certaines de ces traces sont des données à caractère personnel telles que définies par la loi modifiée du 2 août 2002 puisqu'elles portent sur des personnes « *identifiées ou identifiables* »⁴⁶ : en effet, une information du genre adresse IP permet d'identifier son utilisateur. A ce titre, ces données devront faire l'objet de la protection adéquate pendant leur utilisation comme nous le verrons plus tard.

V.2 LES MOYENS TECHNIQUES DE RECOLTE DES TRACES.

Le journal

La plupart de ces traces sont enregistrées dans un journal, plus communément appelé fichier *log* ou *log*. Ces fichiers reprennent dans un ordre séquentiel toutes les transactions passées sur un système, les *events*. Un event correspond à une commande. Ce qui peut faire croire que, lorsqu'on lit un journal, on lit comme dans un livre tout ce qui s'est passé dans notre système. C'est faux. Les journaux présentent des lacunes importantes quant à l'interprétation des événements comme décrits ci-dessous.

La plupart des journaux listent les événements séquentiellement mais sans numéro d'ordre : ceci est une lacune importante au niveau de l'apport d'une preuve car comment être sûr que la trace d'un événement n'a pas été effacée ou modifiée ?

Un autre point faible est que ces journaux listent les transactions (Qui a fait quoi et à quelle heure) mais ne donnent pas d'information sur ce que j'appelle le « produit » de la transaction, c'est-à-dire les données accédées et l'usage qu'il en a été fait.

De plus, un journal ne reprend que rarement les actions en lecture seule : une donnée a-t-elle été lue ? Et pendant combien de temps ?

Enfin, dans une organisation, un système d'information est composé de plusieurs systèmes ce qui génère généralement plusieurs journaux qui, s'ils ne sont pas corrélés, ne donnent qu'une idée incomplète des transactions effectuées.

⁴⁶ PIERRE-BEAUSSE, Cyril. *La Protection des Données Personnelles*, Luxembourg, Promoculture, 2005.

Il est clair que dans ce cas, le contrôle humain se révèle impossible vu les milliers d'événements générés par ces journaux. Il faut avoir recours à des technologies avancées. Voyons ici ce qu'un outil de ce genre peut faire⁴⁷.

Le traçage des actions des utilisateurs au niveau des applications fera apparaître tout comportement anormal, les comportements normaux étant définis dans la politique de sécurité. Cela signifie donc que tant qu'il n'y a pas eu de violation de la politique de sécurité, il n'y a pas d'incident. Ce qui induit la nécessité d'une politique de sécurité forte.

Ce genre de produit génère donc un journal construit en différentes étapes :

- les activités des utilisateurs sont enregistrées de façon à pouvoir être reproduites touche par touche et donc écran par écran.
- le contenu des écrans enregistrés est analysé afin d'identifier les inputs de façon à pouvoir connaître qui a accédé à quoi et ce qui a été fait.
- Génération d'alertes en ligne

Pour ce faire, le trafic est intercepté entre le client et le serveur et chaque paquet -dans chaque sens- est analysé puis classé de manière à pouvoir reconstruire une session utilisateur complète. Tout ceci se passant en temps réel, les alertes le sont également.

Un exemple étant l'employé de banque faisant des recherches par numéro de compte : ce genre de recherche implique des accès répétés et déclenchera une alerte dès que le nombre de recherches permises par la politique de sécurité sera dépassé. Le même processus peut être appliqué à tous les aspects de la politique de sécurité.

Le gros avantage d'un tel système est l'enregistrement touche par touche : le fait de les retaper fera que le scénario complet sera rejoué, permettant ainsi de retracer tout le chemin fait par l'attaquant, en ce y compris les actions *read only*.

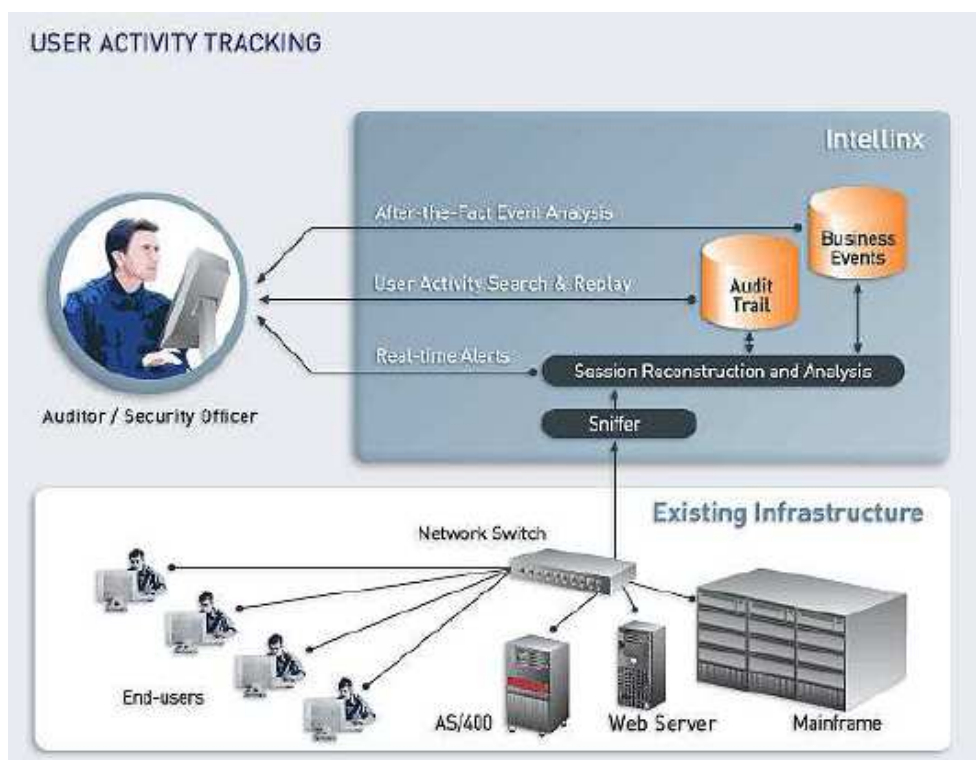


Figure 2 INTELLINX Monitoring Solution Architecture (Source : www.intellinx-sw.com)

⁴⁷ Le produit « *Intellinx* » a servi de base à cette description. Pour les détails techniques : <http://www.intellinx-sw.com> .

Un autre genre d'outil est le **Simple Logfile Clustering Tool (SLCT)**⁴⁸ qui est conçu pour trouver les clusters dans les logs de telle sorte que chaque cluster corresponde à une transaction plus ou moins fréquente. Voici par exemple ce qu'il est capable de détecter :

*Dec 18 * myhost.mydomain sshd[*]: log: Connection from * port **

*Dec 18 * myhost.mydomain sshd[*]: log: Password authentication for * accepted.*

C'est avec ces événements que l'on bâtira un modèle de fichier log afin d'identifier les transactions plus rares qui se différencient du modèle et qui sont de possible anomalies. Ce sont ces anomalies qui feront l'objet d'une investigation.

La récolte des traces de ce qui « n'existe plus ».

Que ce soit l'affaire « *Sarkozy, ClearStream et l'ordinateur du général Rondot* » ou des réseaux de pédophiles confondus, l'actualité met régulièrement en évidence le fait que l'on peut, en informatique, retrouver ce qui a été effacé sur un ordinateur, regarder ce qui a été visionné sur le web ou encore réimprimer la dernière page d'une impression. Cette situation présente évidemment des risques au niveau de la confidentialité de l'information à partir du moment où ce disque se trouve en d'autres mains, en cas de revente ou de mise au rebut par exemple⁴⁹.

Savez-vous ce qu'est un palimpseste ? C'est un manuscrit sur parchemin dont la première écriture a été lavée ou grattée et sur lequel un nouveau texte a été inscrit. Mais il est encore possible de lire ce qui a été écrit auparavant et c'est comme cela que des archéologues ont découvert le *Traité des corps flottants* d'Archimède sur lequel un texte de la bible du XIIe siècle avait été réécrit.

Rien n'a changé. Du moins dans le principe.

Comme dans l'antiquité avec les palimpsestes, « supprimer » en informatique ne signifie pas « faire disparaître ». Nous allons voir comment tout cela fonctionne avec un disque dur⁵⁰.

Un disque dur est en fait composé de plusieurs plateaux empilés les uns sur les autres autour d'un axe. Les données sont stockées sous forme de polarisation puis sont transformées en code binaire par la tête de lecture-écriture qui va les numériser (convertir analogique en numérique). Comme montré dans la figure ci-dessous, les plateaux sont organisés en pistes, cylindres et secteurs. Les pistes sont des sillons gravés à la surface des plateaux : lorsque les données sont localisées sur les mêmes pistes de plusieurs plateaux, on parle de cylindres. Les pistes sont divisées en secteurs. C'est la table d'allocation des fichiers qui définit le statut

⁴⁸ <http://www.estpak.ee/~risto/slct/>

⁴⁹ Lire à ce propos l'article édifiant de Garfinkel et Shelat : <http://web.mit.edu/newsoffice/2003/diskdrives.html>

⁵⁰ Source : Ambroise Soreau, Expert. Avec l'aimable autorisation du CELOG. Créé en 1976, spécialisé dans l'expertise informatique et la preuve informatique, ce centre est composé d'experts ayant une double compétence juridique et technique pour des prestations personnalisées (www.celog.fr)

des clusters (disponible, réservé, défectueux) et qui définit les clusters dans lesquels sera stocké le fichier. Si ce fichier utilise plusieurs clusters, c'est la table d'allocation qui maille ces différents clusters.

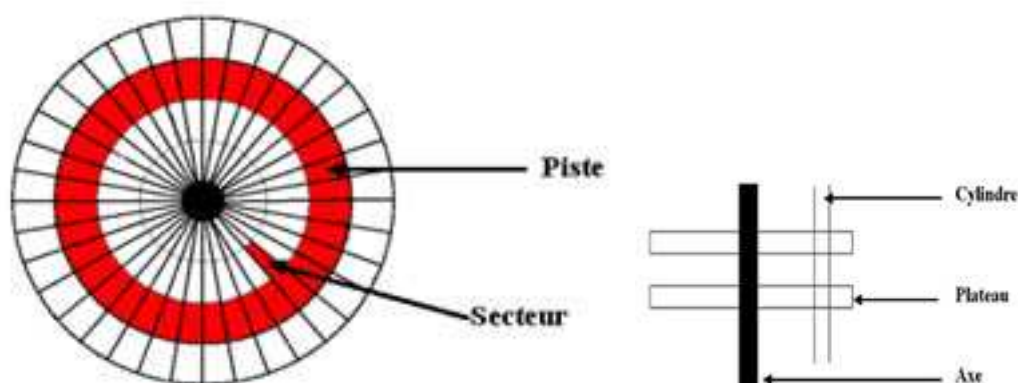


Figure 3 Composition d'un disque dur (Source : Celog)

En fait, lorsque l'on efface un fichier en frappant « Delete », on met seulement à jour une table : la structure du fichier est détruite mais son contenu reste intact localisé dans des blocs non alloués du disque. Le fait de formater un disque ne fait que répéter le processus précédent autant de fois qu'il y a de fichiers

Il faudrait donc réécrire tout le disque de façon à ce que toutes les données soient écrasées.

Mais même dans ce cas, il est possible de récupérer une partie de l'information grâce à des technologies de pointe. Par exemple, *Veeco*⁵¹ crée et fabrique des appareils qui peuvent scanner la surface de disques jusqu'à une mesure de nanotechnologie afin de détecter les traces résiduelles d'informations sur lesquelles on a réécrit d'autres informations. Ceci s'explique par le fait qu'un bit écrit sur un disque est une combinaison complexe de données capturées auparavant. Ce qui fait que si l'on modifie le circuit électronique, les têtes de lecture peuvent révéler des données plus anciennes.

La solution idéale paraît être l'utilisation d'un dégausseur. Mais même dans ce cas il est recommandé d'exercer sept fois ce processus sur un disque afin d'atteindre un résultat⁵².

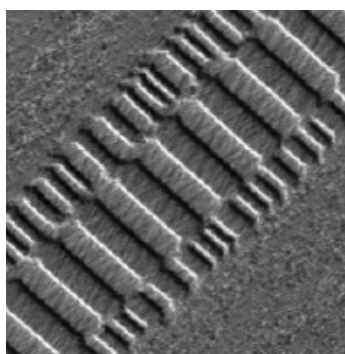


Figure 4 Residuals of overwritten information on the side of magnetic disk tracks.(Source: Veeco)

⁵¹ www.veeco.com

⁵² Cursus formation CISSP (Certified Information System Security Professional)

Mais il me semble évident que ce genre de technologie est réservé à des experts et je ne m'y attarderai pas plus longtemps malgré son aspect passionnant.

Par contre, plusieurs outils permettent ce genre d'investigation. Le plus connu peut-être, abordable par tout qui s'intéresse à ce domaine, une référence mondiale des services de police, s'appelle «*EnCase*»⁵³. Il peut être utilisé sur la plupart des supports fichiers et e-mails pour y retrouver des documents, sur les browsers les plus connus pour retrouver des pages HTML cachées et les images y associées ; il produit des rapports très détaillés et est un standard dans la recherche, la préservation et l'analyse de la preuve informatique.

Cet outil monte les images forensiques en répertoire virtuel « read-only ». C'est donc EnCase, et non le système d'exploitation qui reconstruit le système des fichiers grâce notamment à l'inclusion dans le système d'un outil « write-lock ». De plus, une valeur *hash*⁵⁴ est calculée pour chaque donnée et sera comparée avec l'originale afin de prouver son intégrité. Cela a l'énorme avantage de permettre à l'enquêteur de travailler sur les données de manière non invasive.

Le système permet d'investiguer des objectifs très précis grâce à des outils de recherche très pointus ce qui évite de devoir investiguer tous les documents et autres traces appartenant à la personne incriminée.

La granularité de sa gestion des accès permet de définir précisément ce qu'un enquêteur peut investiguer, à l'exclusion de toute autre choix.

Enfin, le système lui-même produit également un journal qui pourrait servir à prouver devant un tribunal toutes les actions menées par l'enquêteur car il est indispensable pour une entreprise de prouver sa conformité à la loi dans le cas d'une présentation de preuve.

Autres supports.

- Une disquette est structurée de la même manière qu'un plateau de disque dur et permet également de récupérer des fichiers effacés si elle n'a été ni réécrite ni démagnétisée.
- Un disque réinscriptible (CD, DVD) peut lui aussi être comparé à un plateau. Quoique la technologie soit quelque peu différente (différence de température amenée par l'impulsion d'un laser), il dispose également d'une table d'allocation.
- Une clé USB utilise une technologie encore différente appelée « *flash* » (stockage d'électrons) et dispose également d'une table d'allocation qui permet donc la récupération de données.

La récupération de données sur ces différents supports requiert des techniques appropriées.

⁵³ www.guidancesoftware.com

⁵⁴ hash : Une fonction de hachage est une fonction permettant d'obtenir le condensé (en anglais *message digest*) d'un texte, c'est-à-dire une suite de caractères assez courte représentant le texte qu'il condense. La fonction de hachage doit être telle qu'elle associe un et un seul haché à un texte en clair (cela signifie que la moindre modification du document, même un espace, entraîne la modification de son haché). Il doit s'agir d'une fonction à sens unique afin qu'il soit impossible de retrouver le message original à partir du condensé.

La récolte des traces de ce qui « n'existe pas ».

Vous surfez sur Internet et passez de page en page : à chaque fois que vous changez de page, ou est passée la précédente ? Existe-t-elle encore ? A-t-elle d'ailleurs jamais existé ? La réponse est oui. La meilleure preuve en est que certains outils permettent de reconstruire une ou plusieurs pages html visionnées auparavant ou de retrouver une image .jpeg enfouie dans le cache. Ce sont donc des données que l'inforsique permet de récupérer malgré leur volatilité extrême.

Pour reprendre une référence souvent utilisée dans les textes traitant de ce sujet, souvenons-nous du tableau de René Magritte représentant une pipe sous laquelle est écrit « *Ceci n'est pas une pipe* ». C'est en fait l'image d'une pipe. De même, une image sur un écran n'est pas un fichier mais une image créée par différentes couches de matériels et de logiciels. Et donc, chaque couche peut être corrompue par un attaquant.

De plus, l'information reçue sur cet écran est volatile (voir ci-dessous), volatilité encore aiguë par le fait qu'accéder à un fichier change le contenu de la mémoire vive ainsi que l'horodatage des accès au système.

Certains outils comme NetAnalysis⁵⁵ permettent de reconstruire des pages visionnées auparavant ou de retrouver des images .jpeg contenues dans le cache ; il peut servir de viewer pour un outil comme EnCase. Il identifie certains types de sites internet (par exemple pornographiques) ainsi que les critères de recherche utilisés par un criminel : ceci est évidemment radical pour contrer une défense troyenne et démontrer le caractère intentionnel d'un accès à de tels sites.

Qu'est-ce qu'une mémoire ?

On appelle « mémoire »⁵⁶ tout composant électronique capable de stocker temporairement des données. On distingue ainsi deux grandes catégories de mémoires :

- **la mémoire centrale** (appelée également mémoire interne) permettant de mémoriser temporairement les données lors de l'exécution des programmes. La mémoire centrale est réalisée à l'aide de circuits électroniques extrêmement rapides. La mémoire centrale correspond à ce que l'on appelle la mémoire vive. Cette mémoire vive, généralement appelée RAM (*Random Access Memory* ou *Mémoire à accès direct*), est la mémoire principale du système, c'est-à-dire qu'il s'agit d'un espace permettant de stocker de manière temporaire des données lors de l'exécution d'un programme, les processus actifs. En effet, contrairement au stockage de données sur une mémoire de masse telle que le disque dur, la mémoire vive est volatile, c'est-à-dire qu'elle permet uniquement de stocker des données tant qu'elle est alimentée électriquement. Ainsi, à chaque fois que l'ordinateur est éteint, toutes les données présentes en mémoire sont irrémédiablement effacées. D'où l'importance de ne pas éteindre la machine en cas d'investigation.

⁵⁵ www.digital-detective.co.uk

⁵⁶ Merci à www.commentcamarche.net . Document mis à disposition sous les termes de la licence [Creative Commons](https://creativecommons.org/licenses/by/4.0/).

- **la mémoire externe** (appelée également *mémoire physique*) permet de stocker des informations à long terme, y compris lors de l'arrêt de l'ordinateur. Cette mémoire correspond aux dispositifs de stockage magnétiques (disque dur), optiques (CD-ROM) ou mémoires mortes. La mémoire morte, appelée ROM (*Read Only Memory*) est un type de mémoire permettant de conserver les informations qui y sont contenues même lorsque la mémoire n'est plus alimentée électriquement.

La mémoire « flash » est un compromis entre les mémoires de type RAM et ROM. En effet, elle possède la non-volatilité des mémoires mortes tout en pouvant facilement être accessible en lecture ou en écriture. En contrepartie les temps d'accès des mémoires flash sont plus importants que ceux de la mémoire vive.

La mémoire cache (également appelée *antémémoire* ou *mémoire tampon*) est une mémoire rapide permettant de réduire les délais d'attente des informations stockées en mémoire vive. En effet, la mémoire centrale de l'ordinateur possède une vitesse bien moins importante que le processeur. Cette mémoire rapide stocke temporairement les principales données devant être traitées par le processeur.

- La mémoire cache de premier niveau est directement intégrée dans le processeur et se compose du « cache d'instructions », qui contient les instructions issues de la mémoire vive et du « cache de données », qui contient des données issues de la mémoire vive ainsi que les données récemment utilisées lors des opérations du processeur.
- La mémoire cache de second niveau est située au niveau du boîtier contenant le processeur et vient s'intercaler entre le processeur avec son cache interne et la mémoire vive. Ce niveau de cache est plus rapide d'accès que la mémoire vive mais moins rapide que le cache de premier niveau.
- La mémoire cache de troisième niveau est située au niveau de la carte mère.

Il est clair que ces niveaux de cache permettent de réduire les temps de latence des différentes mémoires lors du traitement et du transfert des informations. Pendant que le processeur travaille, le contrôleur de cache de premier niveau peut s'interfacer avec celui de second niveau pour faire des transferts d'informations sans bloquer le processeur. De même, le cache de second niveau est interfacé avec celui de la mémoire vive pour permettre des transferts sans bloquer le fonctionnement normal du processeur.

On l'a compris, tout cela va très vite :

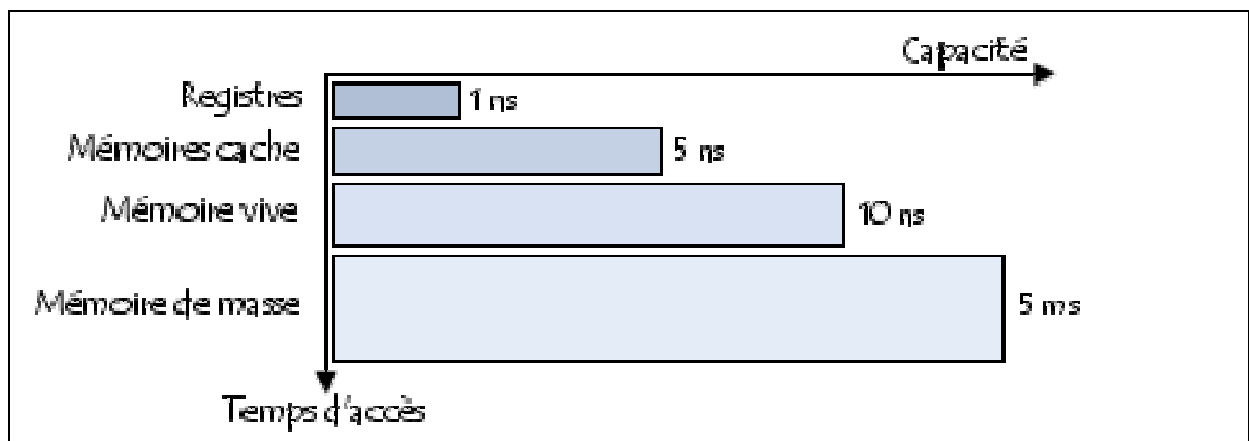


Figure 5 Volatilité et performances d'accès (Source : www.commentcamarche.net)

A la lecture de ce qui précède, il apparaît clairement que capturer et sauvegarder certaines informations relève du défi. C'est cependant possible. Et utile.

Pour pouvoir afficher une page web (HTML), le navigateur doit - à un moment où un autre - avoir le code HTML en clair. Cela signifie qu'il est toujours possible de le retrouver. Comme on l'a vu, la mémoire cache est conçue pour améliorer le rendement du système. Lorsqu'un utilisateur affiche une page web, celle-ci est emmagasinée à la fois dans la mémoire cache du navigateur et celle du disque de l'ordinateur. Quand cet utilisateur veut revoir la page précédente en cliquant sur « Précédent », le navigateur ira la rechercher dans la mémoire cache et non sur Internet.

Cet aspect des choses est important par rapport à l'Art.384 du Code Pénal (Voir note en bas de page 15).

Cela signifie que, tant que le système n'a pas été fermé, l'information est disponible bien que certaines techniques pointues permettent actuellement de retrouver cette information peu après la fermeture du système comme le prouve l'expérience suivante menée à l'université de Princetown aux Etats-Unis : pour ralentir l'effacement des données de la DRAM, on la refroidit alors que l'ordinateur est encore en fonctionnement puis on l'installe dans un autre ordinateur. Ensuite, grâce à un logiciel spécifique, on récupère les données stockées. Parallèlement, les chercheurs ont développé un logiciel permettant de reconstituer des données effacées à partir de celles qui restent⁵⁷.

⁵⁷ <http://www.01net.com/editorial/372376/geler-la-dram-pour-la-faire-parler/>

VI Chapitre cinq : L'application dans l'entreprise

« La sécurité est avant tout une notion d'objectif à intégrer dans l'organisation et la culture de l'entreprise »

-Eric Gheur⁵⁸

Si, comme nous l'avons vu, la technologie permet tout, nous ne pouvons pas nous permettre tout !

Ce chapitre va traiter du contrôle et de la surveillance, deux concepts proches mais cependant bien différents quand il s'agit de l'aspect légal.

C'est à cet aspect légal que seront confrontées les techniques considérées dans le chapitre précédent : comment récolter et utiliser les traces légalement. Nous verrons qu'une certaine organisation facilite les choses.

⁵⁸ Eric Gheur, Expert en gestion de la sécurité, Galaxia I.S.E., Enseignant dans le cursus du Master MSSSI.

VI.1 LES MOYENS JURIDIQUES DE RECOLTE DES TRACES D'UTILISATION

Le traitement de ces traces : contrôle ou surveillance ?

La frontière entre les deux concepts est floue mais faire la différence est primordiale quant à la preuve car, comme on l'a vu, une preuve ne sera acceptable que si elle a été récoltée légalement. L'entreprise a le droit et le devoir de contrôler le travail de ses employés. Elle a également le droit et le devoir de sécuriser les systèmes d'information contre tous les dangers qui les guettent : cela induit donc l'accès et le contrôle des fichiers, des connections et des courriers qui entrent et sortent de l'entreprise, y compris privés.

De l'autre côté, il y a le salarié dont la vie privée – via les fichiers, connections et courriers – doit être protégée. Telles sont les données de la problématique.

La CNPD note que « *Les systèmes évoluent dans des conditions changées, exigeant une sécurisation plus fondamentale et plus efficace. Cette sécurisation ne doit pas se limiter uniquement à l'aspect purement technique, mais elle doit impliquer tous les acteurs concernés (responsables du traitement, employés exécutants et sous-traitants, personnes dont des données sont traitées). Il s'agit donc de combiner des mesures techniques et logiques à des mesures organisationnelles, impliquant une organisation bien structurée, la sensibilisation et la vigilance de tous les acteurs* »⁵⁹

Ce passage est d'importance car il démontre que la CNPD favorisera toujours les mesures préventives de sécurité : si vous remarquez qu'un utilisateur accède à des données auxquelles il n'a pas droit, et bien mettez en place une mesure qui l'empêchera d'agir de la sorte... Il faut noter que c'est également la position du groupe de travail « Article 29 »⁶⁰

Quant à la loi modifiée du 2 août 2002, elle dispose dans son article 22 que « *Le responsable du traitement doit mettre en œuvre toutes les mesures techniques et l'organisation appropriées pour assurer la protection des données qu'il traite contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite* » et insiste sur les mesures de sécurité particulières (Art.23) : « [...] *les mesures visées à l'article 22, paragraphe (1) doivent:*

- (a) *empêcher toute personne non autorisée d'accéder aux installations utilisées pour le traitement de données (contrôle à l'entrée des installations);*
- (b) *empêcher que des supports de données puissent être lus, copiés, modifiés ou déplacés par une personne non autorisée (contrôle des supports);*
- (c) *empêcher l'introduction non autorisée de toute donnée dans le système d'information, ainsi que toute prise de connaissance, toute modification ou tout effacement non autorisés de données enregistrées (contrôle de la mémoire);*

⁵⁹ http://www.cnpd.lu/fr/dossiers/securite_informatique/index.html

⁶⁰ Avis du 29 mai 2002, p.5

- (d) empêcher que des systèmes de traitements de données puissent être utilisés par des personnes non autorisées à l'aide d'installations de transmission de données (contrôle de l'utilisation);
- (e) garantir que, pour l'utilisation d'un système de traitement automatisé de données, les personnes autorisées ne puissent accéder qu'aux données relevant de leur compétence (contrôle de l'accès);
- (f) garantir que puisse être vérifié et constaté l'identité des tiers auxquels des données peuvent être transmises par des installations de transmission (contrôle de la transmission);
- (g) garantir que puisse être vérifié et constaté a posteriori l'identité des personnes ayant eu accès au système d'information et quelles données ont été introduites dans le système, à quel moment et par quelle personne (contrôle de l'introduction);
- (h) empêcher que, lors de la communication de données et du transport de supports de données, les données puissent être lues, copiées, modifiées ou effacées de façon non autorisée (contrôle du transport);
- (i) sauvegarder les données par la constitution de copies de sécurité (contrôle de la disponibilité). »

En pratique, les administrateurs de réseaux « sont conduits par leurs fonctions mêmes à avoir accès à l'ensemble des informations relatives aux utilisateurs [...] »⁶¹. En effet, leurs fonctions consistent notamment à « assurer le fonctionnement normal de ceux-ci ainsi que leur sécurité, ce qui entraîne, entre autres, qu'ils aient accès aux messageries et à leur contenu, ne serait-ce que pour les débloquer ou éviter des démarches hostiles. »⁶²

Selon C.Pierre-Beausse⁶³, il est clair qu'au Luxembourg un tel accès ne peut être effectué que par les personnes normalement compétentes pour assurer la gestion du système informatique et uniquement en vue d'une finalité purement technique. Cela signifie que, par exemple, le Directeur des Ressources humaines ne peut accéder au log afin de s'assurer qu'un utilisateur était bien présent à tel moment. Ou alors il y a changement de finalité et cela devient une surveillance pour laquelle il faut une autorisation de la CNPD.

Considération des cas techniques étudiés auparavant :

Le log : la constitution d'un log est légale si sa finalité est technique. Il contient en effet des informations techniques qui sont le reflet de l'activité du système. Par contre, il contient également des données à caractère personnel et il est donc exclu que celles-ci puissent être exploitées à quelle que fin que ce soit autre que la gestion technique du système puisqu'il s'agit assurément d'une surveillance sur le lieu du travail. Il faut donc que le responsable du système définisse les finalités de ce log et détermine la nature des données dont le traitement permet d'atteindre ces finalités. Il s'agit ici du **principe de proportionnalité** défini dans la loi du 2 août 2002. Comme déjà mentionné, les traces sont inhérentes à l'informatique et une objection majeure est qu'il est impossible d'éliminer certaines données des logs.

C'est encore la CNIL qui nous donne la réponse : « Aussi n'est-ce pas leur existence (NDLR : les traces) mais leur traitement à des fins autres que techniques qui doit être proportionné au but recherché. »

⁶¹ CNIL (Commission nationale informatique et liberté), février 2002.

⁶² Cour d'appel de Paris, 17 décembre 2001.

⁶³ Op.cit.

Dans le cas de l'outil *Intellinx*, le principe du keylogging est assurément de la surveillance et ne peut être mis en place sans autorisation de la CNPD. Il y a donc peu de chance de l'obtenir car la CNPD n'a jamais donné qu'une seule fois ce genre d'autorisation⁶⁴. Depuis lors, silence total, toutes les demandes d'autorisation sont apparemment en attente.

Certains textes mentionnent que l'interception des touches clavier pourrait être assimilée à de l'interception de « correspondance » privée. En l'absence de référence luxembourgeoise, on est enclin à suivre Marie Barel⁶⁵ qui écrit : « *Concernant l'interception des commandes clavier (keystrokes), il convient de souligner que les données sont échangées non pas avec une personne mais bien avec une machine [...]* » ce qui ne permettrait pas d'assimiler ces échanges à de la correspondance privée. Ce cas est à distinguer cependant de l'interception des discussions en ligne pouvant être assimilée à de l'interception de correspondance⁶⁶.

Dans le cadre des techniques inforensiques décrites ci-dessus, il s'agit d'investiguer l'ordinateur d'un utilisateur afin de déterminer et d'identifier une fraude potentielle. Cela implique donc de se connecter physiquement et d'investiguer, ce qui constitue assurément une intrusion dans la sphère privée de l'utilisateur. Il faut donc une autorisation spécifique qui peut être demandée à la CNPD par exprès⁶⁷.

Il semble que la CNPD ait déjà accordé ce genre d'autorisation :

- en donnant l'autorisation de surveiller la personne suspecte à partir du jour où l'autorisation est donnée et sous condition d'informer la personne en question et
- en autorisant l'inspection du disque dur dans l'état où il se trouve au jour de l'autorisation.

Ceci peut prêter à commentaires puisqu'il est probable que la personne se sachant surveillée n'aura plus d'activités répréhensibles et que le disque dur –mémoire physique- contient des informations antérieures à l'autorisation.

Mais peut-être faut-il voir ici une volonté de la CNPD d'entrouvrir une porte en attendant qu'un jour, suite à une plainte, une jurisprudence vienne l'ouvrir entièrement ?

Cependant il faut noter que l'autorisation d'investiguer le disque dur n'autorise pas le viol de la loi, à savoir qu'il ne saurait y avoir accès aux informations privées et donc qu'une investigation « ciblée » devra être menée⁶⁸.

Tout cela n'est malheureusement pas simple et dépend souvent de l'interprétation que font les juges ou la CNPD de la situation. La partie de ping-pong à laquelle se livre actuellement la Cour Supérieure de Justice dans l'affaire dite « *Wagner* » en est la meilleure preuve⁶⁹.

⁶⁴ Cette autorisation est connue sous le nom de « Décision ODYSSEY » et peut être consultée sur www.cnpd.lu/objets/deliberation_73_2005.pdf

⁶⁵ Op.cit.

⁶⁶ Tribunal Correctionnel de Paris, novembre 2000 (www.legalis.net)

⁶⁷ La loi du 2 août 2002 ne vise que les surveillances non occasionnelles

⁶⁸ Voir Chapitre six.

⁶⁹ Voir Annexe 1.

VI.2 QUE PEUT-ON FAIRE ?

S'il est clair que dans l'état actuel des choses il ne sera jamais permis d'accéder à des informations à caractère personnel ou à des informations privées dans le cadre de l'investigation d'une fraude, il n'en reste pas moins que nous pouvons mettre en place une organisation qui permette de maximaliser le champ d'investigation autorisé.

1. Phase 1 : Mise en place

L'Art 11 nouveau de la loi modifiée du 2 août 2002 dispose que « *Le traitement à des fins de surveillance sur le lieu du travail ne peut être mis en œuvre par l'employeur, s'il est le responsable du traitement, que dans les conditions visées à l'article L.261-1 du Code du Travail* »⁷⁰ c'est-à-dire « *2. pour les besoins de protection des biens de l'entreprise, ou 3. pour le contrôle du processus de production portant uniquement sur les machines* ».

L'article 12 cette même loi précise que « (3) *Sont en outre exemptés de l'obligation de notification (ndlr : à la CNPD) ... (k) Les traitements de données à caractère personnel nécessaires à la gestion des systèmes et réseaux informatiques et de communications électroniques, pourvu qu'ils ne soient pas mis en œuvre à des fins de surveillance au sens des articles 10 et 11 nouveau.* »

- ➔ Mettre en place le système ayant pour finalités le contrôle du processus de production et la protection des biens de l'entreprise.
- ➔ S'assurer de la sécurité et de l'intégrité des traces récoltées.

2. Phase 2 : Information des personnes concernées

L'Art.26 de la loi modifiée du 2 août 2002 dispose des modalités de cette information (Se reporter au Chapitre premier).

Le groupe de travail « Article 29 »⁷¹ prône le principe de transparence. Cette information doit être aussi complète que possible et préciser :

- La description du traitement (enregistrement, visionnage, conservation, temporaire ou permanent) ;
- La législation applicable, les sanctions ;

Mais ce dont il faut se rappeler, c'est que l'Art. L.261-1 du Code du travail, Livre 2, Titre VI (Se reporter au Chapitre premier) confère au Comité mixte d'entreprise (ou à défaut les

⁷⁰ Voir Chapitre 1^{er}

⁷¹ Avis du 29 mai 2002, p.15

représentants du personnel) un pouvoir de décision en la matière. Cette information doit donc s'adresser non seulement aux utilisateurs mais à ce Comité mixte.

- Informer les utilisateurs et les représentants du personnel
- Programmes de formation (« awareness »)

3. Phase 3 : Charte d'utilisation

Dans un jugement relativement récent, le Tribunal du Travail de Esch-sur-Alzette⁷² a considéré que « *si en l'absence d'instructions formelles concernant l'utilisation à des fins non professionnelles des outils informatiques, l'employeur doit faire preuve d'une certaine tolérance concernant l'usage à des fins privées des systèmes de communication mis à disposition des salariés, il ne saurait cependant être tenu d'avaliser les abus.* »⁷³

Ce jugement parle donc bien d'instructions formelles qui se retrouveront dans la Charte qui sera un guide *des droits et des devoirs* des utilisateurs, régissant l'utilisation des ressources informatiques et des moyens de contrôle. Porter à la connaissance des utilisateurs les règles d'utilisation est donc nécessaire pour les responsabiliser.

Comme un charte sera écrite dans le respect mutuel des droits et devoirs des employeurs et des employés, il peut être utile de la faire rédiger avec la participation de toutes les parties concernées : délégation du personnel, responsable informatique, direction, RSSI, juriste,...

Elle reprendra toutes les règles d'utilisation des différents systèmes et moyens de communication, les directives de confidentialité, les réactions en cas de suspicion ou d'alerte virale, les sauvegardes, les comportements sociaux, ...

Les administrateurs systèmes ne seront pas oubliés en définissant strictement les limites et conditions de leurs interventions.

Enfin, un effort d'information sera fait quant à la traçabilité et l'imputabilité des transactions dans un système d'information de façon à bien comprendre les contrôles en place.

- Editer une charte et la faire signer.

4. Phase 4 : Organisation du domaine privé

Les informations privées sont contenues dans des fichiers ou e-mails, eux-mêmes contenus dans des répertoires ou autres registres. L'idée est ici d'identifier clairement ce qui est privé de façon à pouvoir investiguer ce qui ne l'est pas. Et pour ce faire, il est conseillé de créer des répertoires intitulés *Privé* ainsi que de faire paraître le mot *Privé* dans l'objet des e-mails. Cette organisation est d'importance pour passer au point suivant.

- Labelliser

⁷² 21 novembre 2003, n°2518 / 2003.

⁷³ Il est intéressant de noter que ce jugement ne tient pas compte et ignore complètement la loi du 2 août 2002 puisque pour identifier un abus, il faut une surveillance.

5. Phase 5 : Conformité avec la CNPD

Malgré tout ce que nous avons vu auparavant, il est conseillé d'adresser à la CNPD une demande d'autorisation préalable de surveillance. Comme expliqué précédemment, cette demande a, à l'heure actuelle, peu de chances d'être acceptée mais elle aura au moins l'utilité de démontrer la bonne foi de l'employeur.

→ Demande d'autorisation⁷⁴

6. Phase 6 : Désignation des responsables

Les administrateurs de réseaux et/ou systèmes doivent être clairement désignés et formés en ce qui concerne leurs responsabilités, leurs obligations légales, leur devoir de confidentialité ainsi que les sanctions prévues par la loi.

→ Formation

7. Phase 7 : Mise en place du contrôle de ces procédures

Il est impératif que toutes ces dispositions soient auditées de façon régulière de façon à être constamment conformes aux lois et règlements. Cette conformité est la condition *sine qua non* pour pouvoir produire des éléments probants en cas de fraude détectée.

→ Outils de surveillance et contrôle

→ Audit

8. Phase 8 : Procédure en cas d'infraction

La découverte d'une infraction ou d'une fraude appelle une réaction. A la lecture de tout ce qui précède, cette réaction –qui sera bien souvent prise « à chaud »– doit être préparée tant au point de vue technique qu'au point de vue légal.

Il nous faut des procédures d'application qui décrivent le processus d'approche des employés dans ces cas d'infraction et qui leurs expliquent leurs possibilités de réaction dans cette situation. A noter que le principe de loyauté évoqué dans la loi modifiée du 2 août 2002 ainsi que préconisé par le groupe « Article 29 » oblige l'employeur à informer l'employé incriminé des résultats des investigations afin que les deux parties puissent confronter leurs versions des faits. A ce niveau, l'employeur a très peu de possibilités.

⁷⁴ Voir en annexe un exemple de demande basée sur une telle organisation.

- Si des doutes existent quand à l'évasion d'information par e-mail, l'employeur peut demander à l'employé incriminé de regarder avec lui les correspondances émises. Le consentement de ce dernier est à ce moment suffisant. Il faut cependant être conscient du fait que si le problème devait aller plus loin, en justice, l'employé pourrait toujours arguer du fait que ce consentement lui a été demandé sous la contrainte et dans ce cas, ce consentement n'aurait plus aucune valeur.
- S'il s'agit d'investigation, par exemple dans les logs, le consentement de la personne concernée ne servirait à rien puisqu'il s'agirait de surveillance sur les lieux du travail et donc soumis à autorisation préalable de la CNPD.

Il est également nécessaire pour l'entreprise de posséder des procédures d'inforsique. Comme le décrit le chapitre suivant, ce processus doit être mené de façon stricte de façon à ce que les résultats soient recevables en justice si nécessaire.

9. En général

Il est utile de rappeler l'importance de la mise en place d'une Politique de sécurité dans l'entreprise car, faut-il encore le dire, l'organisation des ressources est la clé de la sécurité de nos systèmes d'information.

Dans la problématique qui nous concerne, les points suivant sont un minimum à respecter :

- Avant toute chose, considérer l'importance des risques internes.
- L'inventaire et la classification des informations à protéger ainsi que les analyses des risques que courent les systèmes d'information doivent être récurrents. En effet, ces systèmes sont en constante évolution ou, du moins, ont à faire avec des attaquants qui disposent de techniques sophistiquées en constante évolution.
- Les règles de base d'une gestion des accès sont à respecter, c'est-à-dire séparation des tâches, privilèges minima et l'information nécessaire pour travailler (*need-to-know*). De plus, dans ce contexte, apporter un soin particulier à la définition des rôles des administrateurs. Dans ce cadre, instaurer une gestion des arrivées et départs des employés sans oublier les intervenants externes.
- Un programme d'éducation et de sensibilisation de tous les employés et dirigeants est impératif car l'ignorance est également source de problèmes. Il faut prendre en considération les aspects techniques, législatifs et humains.
- Défenses techniques.

VI.3 ROLE DU RSSI

Tout cela peut paraître bien éloigné du monde de l'informatique et de l'information et il paraît difficile de demander au RSSI de maîtriser tous ces domaines.

J'en suis bien conscient et c'est pourquoi je m'en réfère aux résultats⁷⁵ du groupe de travail du CLUSSIL qui, positionnant le RSSI en rapport direct avec la direction de l'entreprise, lui

⁷⁵ « Le RSSI, protecteur de vos informations. Un métier devenu mature ». Document téléchargeable sur www.clussil.lu

donne la possibilité de bénéficier de l'apport de professions plus spécialisées dans les domaines particuliers des lois et de la technique informatiques.

Mais tout cela ne se met pas en place d'un coup de baguette magique ; au contraire, l'entreprise doit se préparer longuement à pouvoir réagir en cas de fraude ou de malveillance. Le rôle du RSSI n'est ici pas anodin : chef d'orchestre de la Politique de sécurité, il ne rechignera pas à jouer le rôle de « canif suisse » et de mettre la main à la pâte. C'est à lui à coordonner la mise en œuvre de toutes ces mesures, soutenu en cela par les dirigeants de l'entreprise.

En matière de traçabilité, journalisation et synchronisation, il est intéressant et utile de s'en référer à la norme ISO 27002 et d'amener l'entreprise à adopter une politique de traçabilité. Cela nécessitera de connaître pour chaque actif le niveau d'exigence du métier et de définir le genre de traces à collecter (simples, détaillées, opposables), et ainsi d'en limiter le volume. A noter qu'en France, cette norme ISO 27001 est opposable en justice.

VII Chapitre six : L'inforensique

« L'inforensique est un art, pas une science »
Alexandre Dulaunoy⁷⁶

Dès lors qu'une fraude est découverte, il est nécessaire de procéder à des investigations afin de pouvoir rapporter la preuve d'une infraction. La preuve étant laissée à l'appréciation du juge, il faut donc mettre toutes les chances de notre côté en respectant tout ce qui a été vu jusqu'à présent. La description ci-dessous n'envisage pas le cas où une plainte est déposée et l'enquête menée par la police : dans ce cas, la direction des opérations lui revient et les policiers appliqueront leurs propres procédures, enquêtant notamment dans le respect du Code d'instruction criminelle.

Il s'agit ici de rassembler les traces contenues dans des systèmes de collecte fiables, dont la finalité a été présentée aux employés, qui ont, si nécessaire, été déclarés/autorisés à/par la CNPD et qui ont été répertoriés dans la charte d'entreprise connue par tous.

Le but est de justifier de la pertinence des preuves trouvées mais également de leur fiabilité : trouver un fichier c'est bien mais prouver des connexions, des échanges, des dates, ... ne fera qu'améliorer la qualité des preuves. Il ne faut pas perdre de vue qu'en sus de la preuve des faits matériels, l'intention elle aussi devra être prouvée.

Enfin, toute l'investigation se déroulera si possible en présence d'un tiers indépendant et les preuves ainsi récoltées seront conservées dans un endroit sûr et protégées de la même manière que toute autre information.

Les supports de l'information sont nombreux : PC et tous autres disques mais également PDA, clé USB, téléphone portable, bandes, machine fax, ... Investiguer sur ces différents supports demande des techniques différentes mais la méthodologie de l'investigation est identique. Le référentiel inforensique présenté ci-dessous est inspiré de deux organisations faisant foi en la matière : l'ACPO et le CELOG⁷⁷.

⁷⁶ Expert en sécurité informatique (Computer Security Research and Response Team (CSRRT)), Enseignant dans le cursus Master MSSSI de l'Université de Luxembourg.

⁷⁷ Merci à ACPO (Association of Chief Police Officers, UK) : document téléchargeable sur www.acpo.police.uk/policies.asp, CELOG (Centre d'expertise informatique français) : document recevable sur demande à www.celog.fr

L'investigateur

Au vu de tout ce qui a été considéré jusqu'à présent, il est clair que la personne qui sera chargée de l'investigation inforensique devra porter deux casquettes : celle d'expert informatique et celle de détective. Dans le cas où cette personne ne possède pas les connaissances nécessaires dans les deux domaines, l'investigation se fera en duo. Le détective déterminera le champ d'investigation et dirigera les recherches de l'expert informatique.

Il permettra de respecter la loi sur la protection des données personnelles en utilisant expérience et sa connaissance du cas afin de déterminer au mieux les pistes (mots clés, types de fichiers, ...) qui permettent ainsi de cibler la recherche et d'éviter au maximum l'intrusion dans des données personnelles de la personne suspectée mais aussi d'une éventuelle tierce personne.

Fixer la scène

En premier lieu, il est utile de réaliser des photos de la configuration, connexions comprises. En effet, il est possible que certains périphériques aient été utilisés afin de commettre la fraude. Si tel est le cas, les traces de connexion se retrouveront dans un log ce qui permettra de connaître l'usage qui en a été fait.

Ne pas fermer ni ouvrir l'ordinateur

Comme nous l'avons vu, beaucoup d'informations peuvent se retrouver lorsque la machine est sous tension alors qu'elles disparaissent avec la mise hors tension. De plus, fermer la machine fera perdre l'information stockée dans des répertoires encryptés. S'il faut cependant la fermer pour la transporter ailleurs, il faut alors couper l'alimentation en retirant la prise car le fait d'utiliser la fonction *off* générera des écritures dans les fichiers et les logs. Pour un ordinateur portable, il est conseillé de retirer la batterie.

De même, le fait d'allumer un ordinateur éteint causera l'écriture de centaines d'informations sur le disque.

Dans certains cas il peut être utile de débrancher d'autres câbles connectés car certains systèmes peuvent être accédés à distance.

Avant de décider de la manière de procéder, il est intéressant de se poser la question de savoir quel genre de trace est recherché. En effet, il est parfois beaucoup plus facile de récupérer la mémoire que de se lancer dans de longues recherches sur un disque.

Journal d'investigation

A partir de cette étape, chaque intervention sera soigneusement consignée dans un journal de façon à pouvoir rapporter devant une instance judiciaire mais aussi de façon à ce que un autre expert puisse éventuellement confirmer ou infirmer les résultats des recherches en rejouant les mêmes investigations.

Je rappelle ici que le témoignage d'un expert fait office de preuve (« *la preuve testimoniale* ») comme décrit dans le Code d'Instruction Criminelle, Art.158.

Imprimantes

Il est élémentaire de vérifier le contenu des bacs des imprimantes connectées au système.

Copier le disque dur⁷⁸

La préoccupation majeure lors de l'investigation d'un PC est de laisser les données inchangées sur le disque et d'en produire une image exacte. Malgré le fait que certains experts émettent des doutes quant à la perfection d'une copie bit à bit (*bit stream image*), il est reconnu que l'irréfutabilité de la preuve s'obtient en clonant le disque dur ou tout autre support. Au Grand Duché de Luxembourg ce procédé est reconnu par la justice⁷⁹.

L'investigation ne se fera pas sur le support original mais sur une copie. Mieux encore, il est conseillé de faire deux copies, la deuxième pouvant servir à une contre expertise, comme backup ou encore comme pièce à remettre à la justice. Il faut noter que, selon ce que l'on cherche, il n'est pas toujours nécessaire de copier le disque en entier.

Toute copie se fera sur un support neuf sous emballage d'origine, éventuellement ouvert devant témoin, non réinscriptible.

Il est clair que la copie d'un disque dur n'est nécessaire que lorsqu'il faut apporter une preuve en justice. Une investigation en ligne pourrait se faire, par exemple, avec « *HELIX* »⁸⁰, un CD bootable qui monte les fichiers en état read-only et ainsi n'altère en rien les données contenues sur le disque.

Mise en quarantaine du support suspect

Comme dans tout film policier ou seuls les services spécialisés de la police peuvent intervenir sur la scène du crime. Il s'agit ici faire de même, et l'ordinateur suspect doit être isolé pour ne plus être utilisé. La preuve sera ainsi protégée contre toute altération ou destruction.

La recherche

A ce stade, je rappelle l'interdiction par la loi d'accéder aux données et informations personnelles. Seule une plainte en bonne et due forme autorisera la police à poursuivre l'investigation.

Les recherches seront menées selon les traces recherchées. Elles peuvent se faire de différentes manières : par nom, extension ou header pour les fichiers. Par chaîne de caractères ou de mots clés pour les contenus. Recherche sur dates. Recherche dans les « swap files » (caches).

Il existe des comparateurs de fichiers qui montrent les différences de contenu entre deux dates et des comparateurs d'image qui permettent de rechercher des images contenant des couleurs proche de la peau humaine afin d'identifier plus rapidement des photos à caractère sexuel.

Ne pas oublier d'investiguer les espaces libres du disque qui peuvent cacher des informations effacées. Ces informations effacées peuvent prouver le délit d'effacement.

⁷⁸ Voir la description de cette opération en annexe 3.

⁷⁹ René MOES. Cours Master MSSI-Cours B4, *L'aspect technique de la preuve*

⁸⁰ www.e-fence.com/helix

Il est évident que la taille des disques actuels ne rend plus possible la recherche humaine. Il faut donc avoir recours à des outils. Il existe beaucoup d'autres outils inforensiques que NetAnalysis ou EnCase précédemment cités. Le problème est que tous ces outils ne sont pas nécessairement adaptés à tous les systèmes d'exploitation. Si EnCase est unanimement reconnu, notamment par la Police luxembourgeoise, il est conseillé de bien se renseigner avant de choisir car le risque de dommage au contenu des supports investigués est réel. De plus certains outils sont plus performants que d'autres, selon la façon dont les données ont été traitées (effacement simple, formatage, dégaussage, ...).

Il faut également disposer d'un éditeur puissant afin de pouvoir lire les différents formats de données qui peuvent être très variés.

Le rapport

Ne perdant pas de vue que ces investigations sont faites dans le but de rechercher des preuves à fournir devant la justice, le rapport sera délivré à des personnes n'ayant pas le même niveau de connaissances informatiques que les experts. Il faut donc que ce rapport soit lisible et compréhensible par ceux qui décideront : à éviter donc les acronymes et autres jargons techniques.

Le rapport devra également répondre aux questions de base : *pourquoi* cette investigation a-t-elle été menée, *comment* elle a été menée et *quelles* conclusions en ressortent ?

La partie la plus importante du rapport est la ou les conclusions. Il faut se garder de tirer des conclusions avant que l'investigation ne soit complètement terminée. C'est ici que l'expérience de l'investigateur va jouer car une (partie de) conclusion incorrecte peut amener la justice à émettre un « *doute raisonnable* » qui bénéficiera toujours à la personne suspectée. ***Les conclusions seront donc des faits et non des supputations*** même si souvent l'expert sera invité à donner son avis.

Le « SANS Institute »⁸¹ permet la consultation d'une méthodologie d'écriture de rapport inforensique (Tous droits réservés).

Rôle du RSSI dans l'inforensique

C'est un aspect du métier qui a rarement été considéré jusqu'à présent puisqu'il n'est guère dans les mœurs des entreprises de réagir de cette façon. Cependant les temps changent et le RSSI pourrait être amené à jouer un rôle dans ce domaine. Lequel ?

En cas de fraude, une réaction rapide est souhaitable. Il faut donc être prêt ce qui signifie avoir des procédures réalistes, qu'elles fassent appel ou non à des interventions externes. Il appartient au RSSI de s'assurer que l'entreprise est bien dotée de telles procédures.

⁸¹ www.sans.org

VIII Conclusions

Arrivé en fin de ce travail, la première conclusion qui s'impose est que tout cela n'est pas simple. Beaucoup d'éléments entrent en ligne de compte et présentent des conflits d'intérêt: technique versus légal, employeur versus employé, privés versus économique.

Lequel de ces éléments doit primer ? La réponse sera différente selon les sensibilités et les responsabilités de chacun. Je me souviens de ce responsable de département s'emportant « *Je n'en ai rien à faire [de la loi], je veux voir le mail qui a été envoyé !* ». Puis-je le blâmer ? Difficile car cette personne, de bonne foi, agit dans l'intérêt de son entreprise. Puis-je pour autant l'autoriser à accéder à une boîte de courrier qui n'est pas la sienne ? Non, bien sur.

Comme souvent répété, c'est l'être humain qui est au centre de cette problématique, lui qui n'est jamais assouvi, qui veut toujours plus et qui, dans cette logique, transporte sa vie privée sur le lieu de son travail. Est-ce acceptable ? Ce n'est pas à moi à donner la réponse mais je me dis qu'il faut rester raisonnable : tout le monde a un jour eu besoin d'un moment de vie privée alors qu'il se trouvait au travail. Mais de là à venir au travail pour s'y consacrer à sa vie privée, il y a un pas que je ne suis pas prêt à franchir. Or, à la lecture de tous ces textes de loi et de jurisprudence, je me dis que ce pas se prépare à être franchi.

Il y a donc menace sur certains secteurs professionnels, spécialement ceux dont l'information est la matière première, le fond de commerce. La technologie a rendu la fuite de cette information si facile que la lutte contre cette délinquance est devenue une part importante des budgets des entreprises. Mais ces budgets, je les compare aux troupes de César qui encerclent continuellement un village gaulois mais qui ne parviennent pas à empêcher les habitants de sortir car ils ont une arme imparable : la potion magique ! Qui donc pariera sur les troupes de César ? Alors que le Grand Duché de Luxembourg ambitionne de devenir le coffre-fort de l'information européenne, il faut bien dire qu'il a également son petit village gaulois qui résiste encore et toujours à la construction complète de ce coffre-fort. Qui donc confierait ses informations à un système qui refuse de voir que les menaces ne sont pas techniques mais humaines alors que nous savons tous que la technique n'apportera jamais toutes les réponses aux besoins de sécurité ? Je plaide ici non pas pour l'abolition des droits des personnes à bénéficier d'une sphère privée dans leur environnement professionnel mais pour un assouplissement raisonnable des règles qui ont été considérées dans ce travail. Je me base pour cela sur l'avis du groupe « Article 29 » déjà cité en page 18 « *Si les salariés ont droit à un certain degré de la vie privée sur leur lieu de travail, ce droit ne doit pas léser celui de l'employeur de contrôler le fonctionnement de son entreprise et de se protéger contre une action des salariés susceptible de nuire à ses intérêts légitimes* ». Dans l'évolution de tout processus, il revient à chacun de prendre ses responsabilités.

La situation est d'autant plus dommage que la législation nationale a évolué et s'est adaptée à la technologie. Le Code Pénal luxembourgeois n'a rien à envier à ses homologues français ou belge et les quelques jurisprudences existantes vont dans la direction généralement prise par nos voisins.

Ceci dit, le monde de la sécurité de l'information est un monde passionnant, un monde en devenir. Il est donc normal que nous soyons en train d'en baliser le chemin. Au Grand Duché de Luxembourg, non seulement nous sentons mais nous voyons les choses bouger. Les

initiatives, privées et publiques, sont nombreuses : la mise sur pied d'un Master en Management de la Sécurité des Systèmes d'Information par l'Université de Luxembourg en partenariat avec le CRP Henri Tudor répond clairement aux besoins de l'ambition du pays et de ses entreprises.

Comme j'ai essayé de le démontrer dans ce travail, ce monde de la sécurité de l'information fait appel à différents aspects technologiques, législatifs, sociologiques et humains et est un réel challenge pour les personnes qui en ont la charge. J'en veux pour preuve la composition du groupe de travail RSSI au sein du CLUSSIL⁸² qui regroupe avocats, techniciens informatiques, auditeurs, responsables de sécurité, consultants, professeurs et fonctionnaires. Il faut espérer que ces personnes seront supportées dans leur démarche par les pouvoirs publics et les décideurs d'entreprise qui prendront pleinement conscience de l'enjeu.

J'espère que ce travail ne m'aura pas seulement aidé à obtenir un diplôme mais qu'il sera utile à la communauté des RSSI et autres acteurs qui ont fait de la sécurité de l'information leur métier. Bientôt une profession ?

⁸² CLU^b de la Sécurité des Systèmes d'Information Luxembourg.

IX Glossaire

Cluster : la zone minimale que peut occuper un fichier sur le disque. Se traduit en français par « unité d'allocation ».

Dégausseur : effaceur magnétique

Hash: Une fonction de hachage est une fonction permettant d'obtenir le condensé (en anglais *message digest*) d'un texte, c'est-à-dire une suite de caractères assez courte représentant le texte qu'il condense. La fonction de hachage doit être telle qu'elle associe un et un seul haché à un texte en clair (cela signifie que la moindre modification du document, même un espace, entraîne la modification de son haché). Il doit s'agir d'une fonction à sens unique afin qu'il soit impossible de retrouver le message original à partir du condensé. Voir également en annexe 3. <http://commentcamarche.net>

Inforensique : Néologisme formé par les mots « informatique » et « forensique ». Action de collecter, conserver et analyser des preuves issues de matériels informatiques en vue de les produire dans le cadre d'une action en justice <http://www.celog.fr>

Polarisation : manifestation de la nature électrique des matériaux. Cette propriété est exploitée pour réaliser des mémoires binaires. Un état correspondra à «0» et l'autre à «1». En raison de la stabilité de ces mémoires, l'information une fois inscrite demeurera définitivement. Ce nouveau type de mémoire est appelé FERAM (ferroelectric random access memory). Pour plus d'informations : http://polyrama.epfl.ch/art_P106_La_memoire.html

RSSI : Responsable de la Sécurité des Systèmes d'Information. Voir à ce sujet : http://www.clussil.lu/tiki-view_articles.php

Téléologie : étude de la finalité.

X Bibliographie et références

Ouvrages

- CALE, Stéphane, et Philippe TOUITOU. *La sécurité informatique, réponses techniques, organisationnelles et juridiques*, Paris, Lavoisier, 2007.
- FENOLL-TROUSSEAU, Marie-Pierre, et Gérard HAAS. *La cybersurveillance dans l'entreprise et le droit*, Paris, Litec, 2002.
- MITNICK, Kevin. *L'art de la supercherie*, Paris, CampusPress, 2005.
- PIERRE-BEAUSSE, Cyril. *La protection des données personnelles*, Luxembourg, Promoculture, 2005.
- PILLOU, Jean-François. *Tout sur la sécurité informatique*, Paris, Dunod, 2005.
- *Le Petit Larousse 2001*, Paris, Larousse, 2000.

Cours & Articles

- Université de Luxembourg, Coursus Master MSSI
 - DULAUNOY, Alexandre, et René MOES. Cours B4, *L'aspect technique de la preuve*.
 - GHEUR, Eric. Cours A5, *Gestion de la sécurité*.
 - HAGEN, David. Cours B5, *Le contexte sectoriel*.
 - PIERRE-BEAUSSE, Cyril, et Pierre WEIMERSKIRCH. Cours A4, *Protection des données à caractère personnel*.
- BAREL, Marie. *Fraude informatique et preuve : la quadrature du cercle ?*, [En ligne]. Adresse URL : <http://actes.sstic.org/SSTIC05/>
- BAREL, Marie. *Honeypot : un pot-pourri...juridique*, [En ligne]. Adresse URL : <http://actes.sstic.org/SSTIC04/>
- GRAHAM J.A. *Le Droit pénal luxembourgeois face aux attaques informatiques*, [En ligne]. Adresse URL : <http://rechtsinformatik.jura.uni-sb.de/>
- HUMBERT, Jean-Philippe. « *Les mondes de la cyberdélinquance et images sociales du pirate informatique* », Thèse pour le doctorat en sciences de l'information et de la communication, Université Paul Verlaine-Metz, 26 octobre 2007, [En ligne]. Adresse URL : <http://www.cases.public.lu/fr/publications/>
- KESAR, Shalini. *Legal issues alone are not enough to manage computer fraud committed by employees*, [En ligne]. Adresse URL : <http://www.jiclt.com/>
- KRAWEZIK, Stanislas. *La recherche de la preuve*, [En ligne]. Adresse URL : <http://actes.sstic.org/SSTIC05/>

- MASCALA, Corinne. *Droit pénal de l'informatique et droit des personnes*, [En ligne]. Adresse URL : <http://www.biu-toulouse.fr/>
- RASCH, Mark. *The Giant Wooden Horse Did It!* [En ligne]. Adresse URL: www.SecurityFocus.com
- ROGER, Laurent. *Antiforensic*, [En ligne]. Adresse URL : http://actes.sstic.org/SSTIC05/Anti_forensic/
- SOREAU, Ambroise. *Suppression de données sur un disque dur*, [En ligne]. Adresse URL : <http://www.celog.fr>
- VENEMA, Wietse. *Forensic analysis*, [En ligne]. Adresse URL : <http://www.porcupine.org/forensics/>
- VENEMA, Wietse. *The persistence of deleted file information*, [En ligne]. Adresse URL : <http://www.porcupine.org/forensics/>

Webographie

- <http://conventions.coe.int>
- <http://eur-lex.europa.eu>
- <http://www.estpak.ee/~risto/slct/>
- www.acpo.police.uk/policies.asp
- www.01net.com
- www.7safe.com
- www.cc.lu
- www.celog.fr
- www.clussil-lu
- www.cnil.fr
- www.cnpd.lu
- www.cnrs.fr
- www.commentcamarche.net
- www.digital-detective.co.uk
- www.ey.be
- www.e-fence.com
- www.honeynet.org
- www.intellinx-sw.com
- www.journaldunet.com
- www.krollontrack.fr
- www.legalis.net
- www.legilux.public.lu
- www.polyrama.epfl.ch
- www.porcupine.com
- www.sans.org
- www.sciencedirect.com
- www.securityfocus.com
- www.veeco.com
- www.virtualegis.com

Autorisations

- Figure 3 « Composition d'un disque dur » reproduite avec l'aimable autorisation de www.celog.fr.
- Figure 5 « Volatilité et performances d'accès » et description de la mémoire mises à disposition sous les termes de la licence « [Creative Commons](https://creativecommons.org/licenses/by/4.0/) » par www.commentcamarche.net.

Entretiens

- DULAUNOY, Alexandre, Computer Security Research and Response Team (CSRRT).
- PIERRE-BEAUSSE, Cyril, Avocat à la Cour, Allen & Overy Luxembourg.
- HAZAN, Emile, Avocat, Expert judiciaire auprès de la Cour Supérieure de Justice de Luxembourg.

XI Annexes

Annexe 1 : Extrait des arrêts des différentes cours dans l'affaire « Wagner »

Annexe 2 : Guide pour la rédaction d'une demande d'autorisation préalable à la CNPD

Annexe 3 : Copie d'un disque dur

XI.1 ANNEXE 1 : EXTRAITS DES DIFFERENTS ARRETS DANS L'AFFAIRE DITE « WAGNER ».

L' « affaire Wagner » est ainsi nommée du fait de la prévention de cette personne d'avoir proféré des menaces sur la personne du Grand Duc à partir d'une cabine téléphonique située dans un bureau de poste sous surveillance vidéo non autorisée par la CNPD malgré la demande d'autorisation préalable introduite par l'Entreprise des P&T deux ans auparavant.

Voici quelques extraits des jugements des différentes cours.

Tribunal d'Arrondissement de Luxembourg, 13 juillet 2006, référence 2523/06

Le Parquet, conscient que l'article 14 (4) de la loi du 2 août 2002 prévoit une peine d'emprisonnement de 8 jours à un an et une amende de 251 à 125.000 euros en cas de violation des dispositions afférentes, estime qu'aucune disposition spécifique de cette loi ne lui interdit d'utiliser les informations ainsi recueillies comme moyen de preuve [...] Il souligne que suivant cet arrêt, le juge pénal peut même prendre en considération une preuve irrégulière dès lors que les dispositions violées ne sont pas prescrites à peine de nullité, que l'irrégularité n'entache pas la fiabilité de la preuve et que l'usage de la preuve n'est pas contraire au droit à un procès équitable.

PAR CES MOTIFS :

Le Tribunal d'arrondissement de et à Luxembourg, neuvième section, **statuant contradictoirement**, les défenseurs de Jean WAGNER entendus en leurs moyens de nullité, le représentant du Ministère Public en ses prises de position :

[...]

d é c l a r e illégale cette preuve obtenue en violation de la Loi;

[Le prévenu est acquitté mais le Ministère public fait appel](#)

Le critère essentiel à examiner est celui qui veut que l'usage de la preuve ne soit pas contraire au droit à un procès équitable. En effet, la Cour considère que le respect de la légalité dans l'administration de la preuve est fondamental pour garantir le caractère équitable du procès.

PAR CES MOTIFS,

la Cour d'appel, dixième chambre, siégeant en matière correctionnelle, statuant contradictoirement, le représentant du ministère public entendu en son réquisitoire et les mandataires du prévenu en leurs explications et moyens,

reçoit l'appel en la forme ;

le dit non fondé ;

partant **confirme** le jugement entrepris ;

Confirmation du premier jugement, c'est-à-dire preuve irrecevable.

Vu l'article 6 alinéa premier de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales contenant notamment l'impératif que la cause du justiciable soit entendue équitablement ;

Attendu que le juge ne peut écarter une preuve obtenue illicitement que si le respect de certaines conditions de forme est prescrit à peine de nullité, si l'irrégularité commise a entaché la crédibilité de la preuve ou si l'usage de la preuve est contraire au droit à un procès équitable ; que ce droit n'est garanti que sous la condition fondamentale du respect de la légalité dans l'administration de la preuve ;

Qu'il appartient néanmoins au juge d'apprécier l'admissibilité d'une preuve obtenue illicitement en tenant compte des éléments de la cause prise dans son ensemble y compris le mode d'obtention de la preuve et les circonstances dans lesquelles l'illicéité a été commise ;

Attendu qu'en refusant de façon péremptoire de prendre en considération tous les éléments de la cause la Cour d'appel a violé la disposition normative susvisée ;

Par ces motifs :

casse et **annule** l'arrêt rendu le 28 février 2007 sous le numéro 126/07 X par la Cour d'appel, dixième chambre, siégeant en matière correctionnelle ;

La cour de cassation refuse que les preuves soient considérées illégales et renvoie donc à la Cour d'Appel.

PAR CES MOTIFS,

la Cour d'appel, cinquième chambre, siégeant en matière correctionnelle et après renvoi suite à l'arrêt de la Cour de cassation du 22 novembre 2007, statuant contradictoirement, le prévenu entendu en ses explications et moyens de défense et le représentant du ministère public en ses réquisitions

déclare l'appel recevable;

le **dit** non fondé;

partant **confirme** le jugement entrepris en ce qu'il a écarté la preuve tirée des enregistrements vidéo réalisés ainsi que tous autres éléments de preuve fondés sur ladite preuve;

confirme encore le jugement entrepris en ce qu'il a déclaré les poursuites dirigées contre Jean Théophile WAGNER irrecevables;

Pour la deuxième fois, la Cour d'Appel a refusé la recevabilité des preuves.

Quelques citations de ces jugements qui concernent la preuve :

[...] il faut encore une fois répéter avec force que dans un Etat de Droit, la fin ne justifie pas les moyens.

[...] Il est incontestable que le principe de la liberté des preuves est de jurisprudence et de doctrine constante et a pour fondement les intérêts supérieurs de la société. L'explication rationnelle résulte du souci de rechercher la vérité en ne limitant pas les moyens qui peuvent la manifester. La Cour de Cassation belge affirme de manière récurrente qu'en matière répressive, lorsque la loi n'établit pas un mode spécial de preuve, le juge du fond apprécie en fait la valeur probante des éléments sur lesquels il fonde sa conviction. Si toute preuve peut

être utilisée, cela ne signifie pas pour autant qu'elle puisse être recherchée ou obtenue de n'importe quelle manière.

[...] Il est à cet égard permis de se demander encore si la production en Justice d'une preuve obtenue illégalement ou de façon déloyale ne méconnaît pas les principes de la Convention européenne des droits de l'homme et du droit au procès équitable.

[...] « aucune juridiction ne peut, sans desservir une bonne administration de la justice, tenir compte d'une preuve qui a été obtenue, non pas simplement par des moyens déloyaux, mais surtout d'une manière illégale. Si elle le fait, le procès ne peut être équitable au sens de la Convention »

[...] la provenance de l'appel téléphonique entré au Palais grand-ducal est intimement, voire indissociablement, liée à la saisie des cassettes vidéo, la Cour ne peut, dans la discussion de l'admissibilité des enregistrements vidéo en tant que moyen de preuve et au regard tant des dispositions de l'article 10 (3) de la loi de 2002 que du principe de la légalité dans l'administration de la preuve posé comme condition fondamentale de la garantie du droit à un procès équitable, faire abstraction des conditions dans lesquelles le moyen de preuve litigieux a en définitive été obtenu.

[...] Dans les conditions données, et alors que de la combinaison de la production en justice d'un moyen de preuve, illicite, [...] il résulte en l'espèce une atteinte au droit à un procès équitable (en tant que ce droit tend au respect des droits de la défense et suppose la légalité de la procédure), qui ne peut pas être réparée au titre du seul débat contradictoire au fond auquel l'appréciation de la fiabilité et de la valeur probante d'un élément de preuve doit de toute façon donner lieu, la décision des premiers juges d'écarter la preuve résultant des enregistrements vidéo réalisés se justifie. Les premiers juges sont encore à confirmer en ce qu'ils ont, par voie de conséquence, déclaré les poursuites irrecevables.

XI.2 ANNEXE 2 : DEMANDE D'AUTORISATION PREALABLE A LA CNPD

Messieurs,

Je vous écris en ma qualité de Directeur général de la société de droit luxembourgeois ENTREPRISE établie et ayant son siège à Luxembourg.

ENTREPRISE envisage de mettre en place un traitement en vue de contrôler l'utilisation par ses employés et collaborateurs (les **Employés**) du courrier électronique, de l'accès à Internet et des systèmes informatiques d'ENTREPRISE (en particulier le disque dur des ordinateurs mis à disposition des Employés) (le **Traitement**).

La mise en place du Traitement est exclusivement motivée par le souci d'assurer le respect des droits et la sécurité des biens d'ENTREPRISE, dans les conditions exposées ci-après.

Considérant que les données recueillies lors du Traitement portent sur des préposés d'ENTREPRISE, la mise en place du Traitement tombe sous le coup de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement de données à caractère personnel (la **Loi**).

Dans ces circonstances, et conformément à la Loi, ENTREPRISE sollicite l'autorisation préalable de la Commission nationale pour la protection des données.

Le traitement envisagé est effectué sous la responsabilité de ...

Le Traitement est légitime au sens de l'article 11 nouveau de la Loi et de l'article L.261-1 du Code du Travail, Livre 2, Titre VI en ce qu'il est nécessaire pour les besoins de protection des biens d'ENTREPRISE.

Information des employés se fera conformément à l'article 11 nouveau de la Loi et de l'article L.261-1 du Code du Travail, Livre 2, Titre VI .

Les finalités du Traitement

L'origine des données

- courrier électronique et accès Internet
- disque dur des ordinateurs

Traitements

- Traitement portant sur le courrier électronique
Description de la mise en place
- Traitement portant sur l'utilisation d'Internet

Description de la mise en place

- Traitement portant sur le contenu des ordinateurs et des disques durs

Description de la mise en place

Catégories de personnes concernées

Quelles personnes sont concernées ?

Destinataire des données

Qui va consulter ces données ?

Pays tiers vers lequel le transfert des données se fera ou pourrait se faire

Maison mère ?

Description des mesures de sécurité

Décrire ici les mesures de protection

Conservation des données

Préciser la durée de conservation des données.

ENTREPRISE demande respectueusement l'autorisation de la Commission nationale pour la protection des données pour le Traitement.

Veillez agréer, Messieurs, l'expression de ma respectueuse considération.

XI.3 ANNEXE 3 : COPIE DU DISQUE DUR

Copier un disque dur à des fins d'inforsique implique que la copie soit 100% fidèle à l'original. Cela signifie que **tous** les paramètres doivent rester inchangés, en ce y compris les paramètres des fichiers comme, par exemple, les dates de création, de dernière écriture ou sauvegarde, Or comme chacun le sait, certains systèmes d'exploitation – et notamment Windows- changent ces paramètres dès l'ouverture.

Il faut donc utiliser du matériel spécial qui empêche cela et qui donc copie en « *write lock* », c'est-à-dire en bloquant l'écriture⁸³. Mais nous ne vivons pas dans un monde parfait et la réussite d'une copie dépend parfois du logiciel utilisé : il n'est pas automatique que tous les outils fonctionnent bien sur tous les systèmes d'exploitation.

D'autres questions se posent, notamment en cas de copie bit à bit. Par exemple, en cas d'erreur sur le disque original, quid de la suite : l'erreur est-elle simplement recopiée ? Quel peut être son influence sur la suite de la copie ? L'erreur pouvait-elle être volontaire ? Et beaucoup d'autres questions auxquelles il est difficile de répondre avec certitude si l'on considère les millions d'informations contenues sur un disque dur.

Mais il nous faut travailler et actuellement les investigateurs s'accordent à dire que ce genre de copie est suffisamment fiable pour être la base du travail d'inforsique. Au Grand Duché de Luxembourg, cette technique est acceptée par les tribunaux⁸⁴.

Hash value

Comme plus tard il faudra prouver que la preuve n'a pas été manipulée de quelque manière que ce soit, il faudra calculer la « *hash value* » de l'image. Cette valeur, traduite en français par *haché* ou *condensé*, est une suite de caractères représentant les données qu'il condense. Cette fonction de hachage est telle qu'elle associe un et un seul condensé à une donnée: changer ne fut-ce qu'un espace ou un point dans le contenu de cette donnée changera son condensé et démontrera que l'information a été altérée. De plus, il s'agit d'une fonction à sens unique ne permettant pas de retrouver la donnée originale à partir du condensé. On peut donc comparer le condensé à l'emprunte digitale de la donnée.

Les algorithmes les plus connus sont⁸⁵ :

- **MD5** (*MD* signifiant *Message Digest*). Développé par Rivest en 1991, MD5 crée une empreinte digitale de 128 bits à partir d'un texte de taille arbitraire en le traitant par blocs de 512 bits. Il est courant de voir des documents en téléchargement sur Internet accompagnés d'un fichier MD5, il s'agit du condensé du document permettant de vérifier l'intégrité de ce dernier)
- **SHA** (pour *Secure Hash Algorithm*, pouvant être traduit par *Algorithme de hachage sécurisé*) crée des empreintes d'une longueur de 160 bits SHA-1 est une version améliorée de SHA datant de 1994 et produisant une empreinte de 160 bits à partir d'un message d'une longueur maximale de 2^{64} bits en le traitant par blocs de 512 bits.

⁸³ Pour quelques exemples: www.celog.fr/disquedur/duplication.htm.

⁸⁴ MOES, René. Cours Master MSSI, Cours B4 *L'aspect technique de la preuve*.

⁸⁵ www.commentcamarche.net. Document mis à disposition sous les termes de la licence [Creative Commons](https://creativecommons.org/licenses/by/4.0/).