Les Infections Informatiques Bénéfiques

Chroniques d'un anathème

Frédéric DUFLOT

DESS de Droit du Numérique et des Nouvelles Techniques
Université Paris XI - Faculté Jean Monnet
Membres du Jury : Me Olivier ITEANU, M. François PAGET

2003-2004

Contact : varenheim@libertysurf.fr

A Dick, Dickson, Gibson, Sterling et Stephenson,

« Le virus chinois se dépliait autour d'eux ; ombre polychrome, innombrables couches translucides qui se modifiaient et se recombinaient. Changeant, énorme, il les dominait de toute sa taille, masquant le vide. »

William Gibson, « Neuromancien »

Plan

Introduction

Avec l'avènement de l'ère numérique, une toute nouvelle forme de criminalité est née et remet en cause les systèmes d'informations, centralisés ou non, des différents acteurs des réseaux et notamment de l'Internet. La question de la sécurité informatique, matière qui tend à protéger ces systèmes d'informations et les données qu'ils hébergent, ne s'est jamais posée avec autant d'acuité. En effet, il ne se passe pas un jour sans que de multiples failles soient découvertes, de nouveaux correctifs développés pour y remédier ou de nouvelles « idées » cybercriminelles apparues, la dernière en date étant la proposition de prestations d'« attaques » informatiques afin de paralyser son concurrent, son voisin ou une institution notoire pendant une période donnée1.

Domaine de professionnels à la pointe de la technique, la sécurité informatique s'aventure parfois parmi les novices et les néophytes. Les virus informatiques font partie de ces rares incursions de la sécurité informatique dans la vie de chacun. Qui n'a pas effectivement maugréé, souvent à tort, devant son écran d'ordinateur contre le dernier virus en date, et dont il a vu un article sur un des forums ou des *blogs* qu'il a visité, en observant un événement informatique dont il ne comprenait pas la cause et, quelques fois, même pas la nature.

Cependant, il n'est pas possible de nier le caractère généralement néfaste des virus informatiques[2]. En effet, ils mettent souvent à mal l'équilibre fragile des systèmes d'informations actuels. En outre, il s'agit d'un risque non négligeable et dont l'avenir des composantes est, semble-t-il, assuré. Si on observe le fonctionnement actuel de l'Internet et la douzaine de systèmes qui servent de référence à tous les autres afin de procéder à la mise à jour de l'ensemble des adresses des serveurs DNS[3] du monde entier ou que l'on s'informe sur les projets TCPA et *Palladium/Longhorn*[4], on s'aperçoit que la centralisation de quelques ressources indispensables à l'informatique moderne fait la part belle aux menaces informatiques, au premier rang desquelles se situe la menace virale.

En effet, si tous les professionnels s'accordent à dire que la plupart des virus actuels est mal conçue, qu'ils disposent eux-mêmes de failles dans leur conception ou leur création, les virus informatiques se trouvent néanmoins, en 2003, avec 35 % des sinistres informatiques causés par une infection informatique virale, en première ligne des incidents informatiques[5]. Il est vrai que

---

[1] Le quotidien russe « *Vedomosti* » publiait le 10 juin dernier un courrier électronique reçu d'un informaticien, louant ses services de blocage de systèmes d'information via une attaque DDos, avec des sommes bien déterminées selon le nombre d'heures et la taille du site : une journée pour 150$ par jour, 1000$ pour le site du Kremlin durant une semaine, 80 000 $ pour celui de Microsoft, etc…

[2] Annie gay, Directeur Général de Sophos France, estime toutefois : « *L'auteur de ce ver [Nachi-B] se prend peut-être pour un Robin des Bois des temps modernes, mais il ne peut pas exister de « bon » virus. Nachi-B infecte sans autorisation les ordinateurs, utilise indûment la bande passante du réseau, du temps CPU et de l'espace disque, et modifie les données et la configuration d'un PC. Un ver peut facilement sortir du cadre pour lequel il a été conçu et provoquer des conflits imprévisibles* ».

[3] DNS : Domain Name Server. Chaque serveur de la Toile est identifié par une adresse dite « IP » de la forme xxx.xxx.xxx.xxx (sous Ipv4) et dont la validité est vérifiée plusieurs fois par jour.

[4] Les projets TCPA (pour « Trusted Computing Plateform Alliance ») de *Intel* et *Palladium/Longhorn* de *Microsoft* visent via, notamment, l'installation d'une puce « *Fritz* » incluse sur la carte mère, à ne permettre le démarrage d'un ordinateur que si l'ensemble des matériels et des logiciels est accrédité par un serveur distant [Voir 1].

[5] « *CLUSIF : Politique de sécurité et sinistralité en 2003* », http://www.clusif.asso.fr.

les mesures de protection ne sont pas toujours adaptées, l'information pas nécessairement communiquée et la menace quelque fois pas réellement prise au sérieux.

Toutefois, il ne faut pas oublier qu'un virus est avant tout un programme, aux fonctions particulières, il est vrai, et qu'en tant que tel, il n'est pas, par nature, nocif. Partant de ce constat de neutralité des programmes d'ordinateur, d'une manière théorique, nul obstacle ne semble empêcher l'existence de virus aux effets indésirables inexistants ou négligeables, des virus que l'on pourrait globalement qualifier de « positifs » même si, à première vue, on peut difficilement concevoir une association entre ces deux mots.

Ainsi, sans prendre la défense systématique du bien-fondé des virus, vers et autres parasites de type informatique, il convient de sortir des quelques préjugés informatiques acquis récemment, et de rétablir certains faits, souvent modifiés ou interprétés de manière pas nécessairement adéquate car, de destructeurs, les virus informatiques pourraient devenir utiles ou même source de création[6].

Les infections informatiques bénéfiques, chroniques d'un anathème

Considérant la définition de l'anathème[7], le thème pourrait paraître racoleur. Le choix du titre l'est sans doute, le sujet beaucoup moins. En effet, il ouvre sur une réalité technique, il est vrai, non consensuelle et souvent objet de débats internationaux houleux, généralement oubliée, quelque fois sciemment, qui, pourtant, n'est pas sans intérêt.

Ainsi, en admettant que l'ingéniosité humaine se transpose de la destruction de système à la création utile, un outil reposant sur une technologie virale pourrait s'avérer extrêmement efficace. On peut ainsi aisément imaginer un programme auto-reproducteur se maintenant lui-même, se dupliquant en des endroits logiques différents, à chaque fois que cela est nécessaire et de manière automatique, rapportant des informations relatives au système à une base de données ou encore effectuant les mises à jour de celui-ci[8]. D'ennemi intime, le programme viral deviendrait le meilleur allié de l'administrateur de réseaux, rendant ses tâches de surveillance et de contrôle plus rapides et plus efficaces.

Pourtant, le virus reste associé à l'idée de parasitisme néfaste. Il est vrai que la plupart de ceux qui sont rencontrés sur la toile sont de cette espèce et que les autres, non néfastes, y figurent dans un état quasi conceptuel. Occulter cette situation n'étant pas d'un grand intérêt, faut-il avoir ce travers de manière inversée et condamner formellement les virus « bénéfiques » parce que, dans leur composante majoritaire, les virus constituent effectivement une nuisance ? Par analogie, a-t-on refusé d'effectuer des recherches en matière nucléaire parce qu'Oppenheimer et son équipe

[6] Citons, à titre d'exemple, l'exposition graphique *Viral Counter Attack* de Joseph Nechvatal et du collectif *Music2eye* qui présentait des virus « dévorant » des œuvres de l'esprit ; http://www.viralcounterattack.net/

[7] A savoir, initialement, une excommunication majeure prononcée contre les hérétiques ou les ennemis de la foi catholique (Dictionnaire « *Le Petit Robert », tome 1).*

[8] Une possibilité intéressante d'utilisation d'un code viral serait, dans le cadre d'un logiciel vendu pour une certaine durée ou un certain nombre d'utilisation, la recherche et l'éradication de tout éléments composant ce logiciel (fichiers, entrées dans la base de registre…), de manière bien plus efficace que les systèmes actuels concernant les versions de démonstration ou les « *sharewares* ».

avaient découvert la bombe éponyme, d'utiliser le métal parce que les premiers objets qui furent façonnés avec étaient des armes ? A contrario, l'exclusion d'un terrain de recherche ne permettrait pas de rendre le risque viral moins effectif.

Toutefois, partant de ce constat éminemment théorique, se pose la question de savoir si effectivement, les virus « positifs » ou plus globalement les infections informatiques « bénéfiques » peuvent exister, tant techniquement que juridiquement, ou encore socialement. A ce titre, il convient de déterminer plus précisément l'objet de notre étude.

Alors même que les programmes viraux commençaient à apparaître, le terme de virus n'était pas encore utilisé. Aucune formalisation technique et encore moins juridique n'y était attachée. En effet, le terme de « virus » est pour la première fois utilisé en 1986 dans les travaux du mathématicien et informaticien Fred Cohen, et plus particulièrement sa thèse de doctorat[9], dans laquelle il leur donne cette définition, aujourd'hui admise par tous :

« *Un virus est une séquence de symboles qui, interprétée dans un environnement donné (adéquat), modifie d'autres séquences de symboles dans cet environnement, de manière à y inclure une copie de lui-même, cette copie ayant éventuellement évoluée.* »[10]

De cette définition formelle et difficilement compréhensible ressort l'aspect majeur des virus informatiques, à savoir, leur fonction de reproduction, fonction qui s'accomplit de manière parasitaire par rapport à un programme préexistant, sans référence à une autre fonctionnalité. En effet, il n'est nulle part fait mention d'un quelconque autre effet et, particulièrement, celui que l'on attendrait d'un tel programme quand le terme de virus est utilisé, à savoir, un effet nuisible dans un environnement hôte. Il résulte de cette définition que le fait de ne considérer les virus que sous un angle « diabolique », étranges programmes créés afin de bouleverser la vie informatique des entreprises et des utilisateurs, est réducteur et occulte une partie non négligeable de la définition de Cohen. Cependant, si le terme de « virus » couvre tout code doté d'une capacité d'auto-reproduction, la notion est aujourd'hui plus étroite et plus ample à la fois. En effet, d'une manière générale, il désigne l'ensemble des infections informatiques mais les professionnels les considèrent seulement comme une partie de ceux-ci, voire comme une des deux classes d'organismes viraux informatiques[11].

Le terme d'« *infection informatique* », quant à lui, est issu des travaux d'Adleman publiés en 1989[12] dans lesquels il définit, quant à lui, le mécanisme viral à travers ses deux propriétés

[9] Fred Cohen, « *Computer Viruses* », PhD, Université of Southtern California, janvier 1986.
[10] En version originale : « … *a programm that can « infect » other programms by modifying them to include a possibly evolve copy of itself* ».
[11] Vesselin Bontchev, chercheur au *Virus Test Center* de l'Université de Hambourg, observe par ailleurs que seront considérés par cette définition comme des programmes viraux un compilateur qui compile son propre code source, un gestionnaire de fichier qui réalise une copie de lui-même ou le programme « diskcopy » s'il est utilisé sur une disquette contenant un système d'exploitation [Voir 2]. On remarquera cependant que ces exemples correspondent à des programmes spécifiques dont la fonctionnalité peut être analysée en une réplication. Il ne s'agit pas d'une caractéristique inhérente au type de programme en cause ;
[12] Léonard M. Adleman, *"An abstract Theory of Computer Viruses. In advances in Cryptology"* [Voir 3].

principales, à savoir que tout programme possède une forme infectée[13] et que chaque programme infecté agit selon trois possibilités : une infection, une imitation (le programme infecté fonctionne de manière légitime) ou une fonctionnalité ajoutée. Dès lors que cette fonctionnalité ajoutée, dépendante de l'infection initiale et non du programme infecté, dénote un caractère positif, nous pourrions parler d'infection informatique bénéfique, ce qui peut paraître antinomique mais n'est, en fait, dans notre démonstration, que la précision de la nature de cette fonctionnalité ajoutée.

Par ailleurs, Outre-Atlantique, le terme utilisé pour englober l'ensemble des programmes d'origine virale à vocation malicieuse est celui de « *malware* »[14], terme très pratique car connotant fortement un effet nuisible. Dans le cas qui nous intéresse présentement, le terme inverse de « *goodware* » pourrait être aisément utilisé. Par ailleurs, nous noterons que le terme d'« inoculation » nous semble plus adéquat pour traiter le sujet, mais, le thème étant relativement technique, un minimum de respect du vocabulaire utilisé dans le secteur de la sécurité informatique nous paraît indispensable pour une meilleure compréhension. Nous utiliserons donc le terme d'« infection ». En outre, nous utiliserons parfois l'expression de « virus » pour traiter des mécanismes auto-reproducteurs d'une manière générale. En dernier lieu, nous parlerons de virus « bénéfique » plutôt que de virus « *utile* » pour marquer l'opposition avec les virus au sens général du terme.

Ces quelques précisions sémantiques étant effectuées, rappelons brièvement l'historique de ces virus car, si ces dernières années leur ont été propices, de quelque sorte que ces virus soient, le phénomène n'est pas récent et repose sur des bases aujourd'hui anciennes, en des heures où l'on ne pouvait appréhender ni même imaginer leurs incursions actuelles hors des sphères traditionnelles des informatiques domestiques et professionnelles.

Pour commencer sur les fondements théoriques, il est utile de préciser que la formalisation des mécanismes viraux réalisée par Cohen et Adleman utilise essentiellement les concepts développés dans les travaux de Alan Türing de 1936, et plus particulièrement ceux relatifs à la « *machine de Türing* »[15] ainsi que ceux des théories de l'autocopie de logiciels et des automates cellulaires de John von Neumann de 1949[16]. Ces résultats mathématiques suffisant à la réalisation des premiers virus, ceux ci apparurent, de manière officielle, dans les années 1960.

Le terme de virus n'était alors pas encore utilisé mais la notion de programmes « offensifs »[17] était déjà connue. Les premières recherches ont été ainsi menées en ce domaine et le jeu « *Darwin* », connu ultérieurement sous le nom de « *CoreWars* » est apparu en 1962 au sein des

---

[13] Le virus, dès lors, peut être considéré comme le traitement d'une donnée (le programme sain) pour obtenir une autre donnée (le programme infecté).

[14] Le terme de « *malicious logic* » est aussi utilisé. Pour plus d'informations, se référer à la FAQ *Virus*-L/*comp.virus* ou le forum de news USENET « *comp.virus* » [Voir 4].

[15] C'est à dire la représentation abstraite et générale d'un ordinateur et des programmes susceptibles d'être exécutés sur cet ordinateur, et notamment les virus via leur fonction d'auto-reproduction (Alan M. Türing, « *On Computable numbers with an application to the Entsheidung problem*", 1936 [Voir 5]).

[16] La seconde théorie visait à trouver un modèle réductionniste pour décrire les processus d'évolution biologique et en particulier celui de l'auto-reproduction. (John von Neumann, "*Theory and Organisation of Complicated Automata",* 1949 et *"Theory of Self-reproducing Automata",* 1966 [Voir 6]).

[17] Plus particulièrement des chevaux de Troie utilisant un virus comme vecteur de transmission.

laboratoires de la société *Bell* AT&T. Il s'agissait, pour des « organismes », selon un mécanisme très « darwinien », d'assurer simplement leur propre « survie » par rapport à d'autres programmes, au sein d'un même espace mémoire limité. Le système d'exploitation n'offrait pas de protection entre les espaces mémoire des différents programmes, aussi leur était-il possible de s'agresser mutuellement pour essayer de détruire leurs concurrents. Les algorithmes mis en oeuvre à cette occasion étaient traduits dans un langage d'assemblage spécialement conçu pour l'occasion, le « *red code »*, exécuté via un émulateur. Au fur et à mesure des intervenants, les programmes étaient améliorés au point de détenir un potentiel de destruction qui leur fit arrêter le projet.

Issu d'une simple curiosité scientifique, au même titre que les algorithmes génétiques, ce jeu a néanmoins abouti à la réalisation, par plusieurs personnes, de portions de code capables d'auto-réplication, s'accrochant au secteur de démarrage des disquettes ou aux fichiers exécutables, tout d'abord sur ordinateurs *Apple*, puis PC. Ainsi, en 1983, le virus « *Elk Cloner* » fait son apparition sur AppleDOS 3.3.

En 1986, alors que les travaux de Cohen étaient publiés, était créé le virus de *boot*[18] publicitaire pakistanais « Brain »[19]. A cette époque, la contamination s'effectuait par disquette 5''1/4[20] et était encore très limitée. A titre d'exemple, le virus « *Brain* » n'est jamais sorti des quelques universités américaines où il s'était propagé.

Parallèlement, le programme « *Xerox* », devenu de manière incidente ce que l'on appelle aujourd'hui un ver, apparaît quant à lui en 1981, la même année qu'un virus pour *Apple II.*

La première attaque connue[21], intervenue du fait du ver Internet, le 2 novembre 1988, échappa, semble-t-il, au contrôle de son concepteur et exploita nombre des failles que comportait l'Internet de l'époque, l'aspect nuisible du ver, sans charge finale, se manifestant par une forte surcharge des systèmes infectés.

A quelques exceptions près, les virus n'étaient alors que le fruit d'un accident logique, d'une expérience informatique qui avait mal tourné ou d'essais visant à créer une sorte de vie artificielle[22] autonome et dont l'esprit se retrouve dans le terme même de virus. Néanmoins, il était démontré que l'ensemble des plates-formes informatiques pouvait être touché.

Alors que le monde découvrait les effets qu'ils pouvaient engendrer, la création de ce type de programme se criminalisait, l'effet néfaste devenant la finalité même du programme. Cette pratique restait toutefois artisanale, les créateurs cherchant plus le « plaisir du jeu » et la reconnaissance qu'un véritable profit. Selon M. Paget, « chasseur de virus » pour *Network*

[18] Secteur d'amorce des supports magnétiques et optiques.
[19] La légende dit qu'il a été écrit pour essayer de stopper le piratage des logiciels des deux concepteurs, gérants d'un magasin d'informatique au Pakistan. Il était en effet largement distribué avec les copies illégitimes de leurs logiciels.
[20] Ce format correspond aux disquettes souples de 360 Ko, le format actuel de 3''1/2 étant rigide et contenant 1.44 ou 2.88 Mo.
[21] Le ver *Creeper* (1971*)* n'était effectivement resté qu'au stade d'une expérience sur le réseau Arpanet.
[22] Pour notre étude, nous définissons la vie artificielle comme l'activité de systèmes synthétiques qui exhibent les caractéristiques comportementales de systèmes vivants.

Associates (éditeur de la gamme de logiciels de sécurité *McAfee*), la tendance se serait inversée et laisserait voir une diminution des motivations ludiques originelles au profit des motivations criminelles à la mi-2003[23].

Aujourd'hui, parmi les infections informatiques les plus connues, on peut citer évidemment les virus et vers *Tchernobyl* (1998), *I LoveYou* (1999), *Magic Lantern* (2001)[24], *Blaster* (2003) et *Mydoom* (2004), ainsi que le cheval de Troie/Accès caché *BackOrifice* (2000).

L'actualité virale est encore aujourd'hui techniquement très riche, les programmes malveillants n'ont jamais été aussi nombreux à poindre leurs antennes numériques sur les réseaux[25] et leurs capacités semblent de plus en plus abouties. Pour ne citer que quelques-unes d'entre elles, parmi les plus récentes, le virus *Zafi-B* disposait de la capacité de se présenter dans la langue de l'ordinateur infecté, améliorant ainsi sa technique d'ingénierie sociale et le ver *Atak* d'une protection qui lui permettait de se désactiver dès lors qu'il était manipulé et, donc, de rendre plus difficile son analyse.

Par ailleurs, l'informatique domestique propriétaire n'est pas la seule victime des phénomènes viraux, l'informatique libre les connaît aussi, dans une moindre mesure, il est vrai ; mais aussi les nouveaux produits numériques embarqués tels que les téléphones portables et les assistants personnels numériques. En effet, le 16 juin dernier, le virus *Cabi*r[26] infectait pour la première fois les systèmes d'exploitation *Symbian* des téléphones portables via leur liaison sans fil *Bluetooth*[27] tandis que le 20 juillet, apparaissait *WinCE4.Duts*, le premier des virus pour *Windows CE/Windows Pocke*t *PC*, un des deux systèmes d'exploitation utilisés sur les assistants personnels numériques.[28]

Les virus informatiques présentent clairement un risque dont la conscience du caractère dangereux et néfaste est encore imparfaite. A ce titre, il convient d'informer et de former. Le but de cette étude est de participer, dans une minuscule mesure, à cette œuvre. Toutefois, il est des thèmes que nous n'aborderons pas. En effet, celui de la protection des virus informatiques par le droit d'auteur ne nous paraît pas pertinent dans le cadre de la question que nous voulons résoudre

---

[23] Sans que cela soit soit véritablement significatif, la proportion, en 2004, est à peu près de 40/60, ceci étant principalement dû à l'intervention des très nombreuses versions du virus *Netsky*, développé par un étudiant allemand, Sven Jaschan, déjà auteur de *Sasser* et arrêté le 7 mai dernier. Il s'est fait embauché par *Securepoint* en septembre 2004.

[24] Dans le cadre du projet « *Cyberknight* », le FBI a développé un ver espion nommé « *Magic Lantern* » qui installerait un cheval de Troie de type « *keylogger* » afin d'obtenir des mots de passe et clés de chiffrement de manière plus facile que par les moyens de cryptanalyse classique (Eric Filiol, « *La lutte antivirale : techniques et enjeux* », MISC janvier-février 2003).

[25] Selon l'éditeur de logiciels *Sophos*, au dernier semestre, il y a eu 4677 nouveaux virus, soit 21% de plus qu'en 2003, pour un total avoisinant les 80 000. En 1995, toutes plate-formes confondues, il en existait moins de 6 000.

[26] Le virus *Cabir*, comme de nombreux autres, est un virus dit « *proof-of-concept* », c'est-à-dire un virus créé pour démontrer un concept, une idée, en l'occurrence le fait qu'aucun système et aucune technologie n'est à l'abri d'une attaque virale.

[27] La technologie *Bluetooth* est une technologie sans fil à courte distance (initialement 10 mètres et aujourd'hui jusqu'à 100 m avec le matériel adéquat.) qui ne nécessite aucune configuration préalable particulière.

[28] Ces deux virus avaient un concept assez similaire : il s'agissait de deux programmes créés afin de démontrer, selon leurs auteurs, les failles des deux systèmes d'exploitation. Ils ne disposaient d'aucune charge néfaste particulière.

au final, à savoir, si tant est qu'elle puisse exister en pratique, comment admettre, techniquement, juridiquement et socialement une infection informatique bénéfique.

En effet, les virus sont, sans nul doute, des programmes d'ordinateur et, à ce titre, protégés par le droit d'auteur, sans considération d'une quelconque éthique dans la protection. En tout état de cause, la mise en œuvre de cette protection serait actuellement presque un cas d'école, uniquement réservé à un auteur n'ayant jamais diffusé son œuvre (au sens viral de la diffusion) et par conséquent n'ayant causé aucun dommage[29]. L'intérêt de la protection serait tout autre en cas de possibilités d'exploitation commerciale de ces programmes, mais nous n'en sommes pas encore au stade de la valorisation de ces mécanismes viraux.

Probablement, le premier état d'un organisme artificiel doué de vie[30], dans l'espoir de démontrer l'utilité des mécanismes viraux bénéfiques et de leur nécessaire appréhension juridique par une autre matière que le droit pénal, nous allons nous attacher à les étudier autour de quatre axes : la compréhension de la matière technique (Partie I, Section A), le cadre juridique actuel (Partie I, Section B), son application à la notion de « virus positif » (Partie II, Section A), ainsi que la proposition de solutions, d'alternatives afin de les appréhender d'une manière qui puisse nous les rendre véritablement utiles, à l'opposé des réalisations et des préconçus actuels (Partie II, Section B).

En vertu de ceci, nous analyserons tout d'abord les virus dans un cadre global, sans considération de la finalité de ces codes malicieux (Partie I) avant d'étudier plus précisément les infections bénéfiques (Partie II).

[29] On pourrait par ailleurs se poser la question non pas de l'opportunité de la protection mais de celle de la nécessité d'une autorisation pour reproduire le logiciel alors que celui-ci a pour composante première cette même reproduction, généralement non autorisée.

[30] Les biologistes considèrent que l'unique caractéristique commune à toute forme de vie est leur capacité à se reproduire, quasiment à l'identique, au travers des générations.

Première partie - Du « virus » médiatique aux infections juridiques

La notion médiatique et grand public de « virus » est certainement la plus connue des néophytes en matière de sécurité informatique. Elle couvre cependant une réalité bien plus complexe qu'il n'y paraît d'un premier abord. Dès lors, avant même de s'attacher au régime juridique s'appliquant aux « virus » (Section B), il va s'agir de les soumettre à une analyse technique afin de les caractériser précisément (Section A).

Section A - Analyse technique des phénomènes informatiques offensifs

Sous couvert de ce terme existent de nombreuses sous-catégories, de nombreuses techniques virales s'y rapportant, toutes impliquant des risques différents et donc des mesures de protection diverses. Nous avons vu précédemment que, dans l'esprit du public, le terme de « virus » recoupe l'ensemble des programmes offensifs qu'il pourrait être amené à rencontrer, voire même la globalité des désagréments informatiques qu'il pourrait avoir. A la lueur de la définition pratique des infections informatiques (1), nous allons donc analyser l'ensemble de ces programmes offensifs, tout d'abord en les distinguant les uns des autres (2), puis, pour les plus complexes, objets de notre étude, en rappelant leurs caractéristiques essentielles (3).

1. Définitions et concepts de base

L'expert en sécurité informatique Eric Filiol[31] définit l'infection informatique comme « *un programme simple ou auto-reproducteur, à caractère offensif, s'installant*[32] *dans un système d'information, à l'insu du ou des utilisateurs, en vue de porter atteinte à la confidentialité, l'intégrité ou la disponibilité de ce système ou susceptible d'incriminer à tort son possesseur ou l'utilisateur dans la réalisation d'un crime ou d'un délit* ». Cette définition est à la fois plus large et plus restrictive que la définition des virus par Fred Cohen. En effet, elle intègre les programmes simples, absents de cette dernière, mais aussi un lien, semble-t-il nécessaire, avec les notions de nuisance et de comportements répréhensibles. Nous noterons toutefois l'absence d'un élément en relation avec ces deux notions. En effet, derrière la terminologie d'« *infection informatique* » se cache le concept de parasitisme : les codes malicieux se greffent à un programme ou à un système hôte avec lequel ils interfèrent avec plus ou moins d'autonomie, en fonction du type d'infection concerné.

En tout état de cause, le bon fonctionnement d'une infection informatique suppose deux éléments. Le premier est un élément à caractère technique : le programme infecté « transporte » le programme infectant au sens strict, c'est-à-dire la seule série d'instructions correspondant à l'infection. S'il s'agit de la première infection réalisée par l'attaquant, ce programme infecté est nommé « *largueur* » (ou « *dropper* »). Lorsque ce dernier est exécuté, le programme infectant réagit, prend la main de manière transparente pour l'utilisateur et agit selon ses propres instructions, le programme hôte l'hébergeant étant temporairement placé en état de sommeil. Une

[31] Eric Filiol, « *Les virus informatiques : théorie, pratique et applications* », [Voir 7].
[32] Au vu des développements qui vont suivre, il est nécessaire de bien comprendre le terme d'« installation ». Cela comprend, en effet, une mise en place du code malicieux aussi bien postérieure à celle du logiciel lui-même qu'au même moment.

fois cette finalité accomplie, le programme hôte s'exécute alors normalement sans trahir la présence du programme infectant.

Parallèlement, un élément social est aussi indispensable. En effet, les infections informatiques sont toutes basées, à des degrés divers, sur l'ingénierie sociale. A un moment ou à un autre de l'infection, il y a une imprudence de l'utilisateur qui exécute un fichier inconnu, un programme d'apparence anodine, ludique ou à tout le moins attractif.

De plus, précisons, d'une part, qu'un aspect important des infections informatiques est leur propension à se servir des nombreuses vulnérabilités logicielles, indépendantes des utilisateurs, afin de se propager (nul doute que sans celles-ci, les programmes « malfaisants » seraient bien moins nombreux) et, d'autre part, que la viabilité de chaque infection informatique est liée à un ensemble de caractéristiques techniques déterminant l'environnement dans lequel elle va s'introduire (processeur, mémoire vive ou de masse, système d'exploitation). Il apparaît donc qu'il existe une certaine dualité des vulnérabilités et des virus, les unes autorisant les autres et ces derniers révélant les premières.

Ces concepts fondamentaux étant rappelés, distinguons maintenant les diverses catégories d'infection informatique.

2. Nomenclature des infections informatiques

Si la finalité de cette analyse est clairement de s'attacher à l'appréhension juridique des mécanismes auto-reproducteurs informatiques, il nous semble inepte de ne traiter que ceux-ci. En effet, en matière de sécurité informatique, la classification n'est pas toujours aisée et des programmes vont être référencés, par certains observateurs, dans les virus et, par d'autres, dans les vers, sans qu'une décision définitive puisse être prise. Source de confusion dans l'esprit de l'utilisateur novice, un programme offensif unique pouvant s'appuyer sur plusieurs mécanismes distincts[33], il convient d'opérer une première distinction avec, d'une part, les infections informatiques simples (a) et, d'autre part, les infections informatiques auto-reproductrices (b), chaque catégorie pouvant fonctionner de manière autonome ou couplée avec des éléments de l'une ou l'autre.

a. Les infections simples

Il s'agit de programmes simples dotés d'une fonctionnalité appelée à se déclencher à un instant donné, selon un critère donné (ou « *trigger* »)[34]. Il n'y a pas véritablement de propagation, le programme ayant pour but de se placer ou de s'installer simplement dans le système, et devant être introduit dans le système cible de manière volontaire ou non. Présent en un seul exemplaire,

[33] Contrairement à ce que certains croient, ces fléaux existent d'ores et déjà aussi bien en matière de logiciels propriétaires qu'en matière de logiciels « libres ». Certes, ils trouvent en ces derniers un terrain moins propice à leur développement que sous MS-Dos par exemple, mais il ne faut pas pour autant négliger les dangers présents et potentiels.

[34] M. François Paget, quant à lui préfère préciser qu'il s'agit de « *fonctionnalités malveillantes* » : http://www.clusif.asso.fr/

il s'active généralement par l'exécution d'un fichier du fait de l'utilisateur. Une fois sa finalité accomplie, il se désactive et n'est donc pas résident en mémoire[35].

- Les bombes logiques

La bombe logique est un programme contenant une fonction cachée généralement associée à un déclenchement différé qui va lui permettre, en fonction d'un événement déterminé à l'avance (délai, présence ou absence d'une donnée, de réponse à une commande, …), d'exécuter sa fonction offensive. Cette fonction aux effets très divers[36] est généralement rajoutée de façon illicite à un programme hôte qui conservera son apparence anodine et son fonctionnement correct jusqu'au moment choisi par le programmeur malveillant. Nous noterons qu'il s'agit de la seule infection dont le but unique est de nuire. A ce titre, elle constitue assez fréquemment la charge finale (ou « *payload* ») d'un autre programme simple ou auto-reproducteur (cf. infra II/A/3/a).

- Les chevaux de Troie

Au même titre que la bombe logique, le cheval de Troie informatique, de la même manière que celui qui participa à la prise de Troie par les Grecs approximativement au XIème siècle avant JC et relaté par Homère dans l'« *Iliade* »[37], comporte également une fonctionnalité cachée. Sa mise en oeuvre est toutefois immédiate et systématique car cela est de l'essence même de ce type de programme. Se dissimulant au sein d'une application *a priori* inoffensive et souvent attractive, il se décompose en un élément « serveur », installé dans le système hôte, et un élément « client », qui permet à un utilisateur externe la prise de contrôle à distance de ce système, et, par conséquent, l'exécution de certaines tâches « malignes » et notamment l'insertion d'une bombe logique (contrairement à un virus ou un ver où l'hypothèse de l'insertion de la bombe logique se situe au niveau de la conception du programme ; en ce cas, cette insertion s'effectue après l'activation du cheval de Troie).

Les leurres, programmes imitant le fonctionnement normal d'un programme légitime du système, et « *sniffer* » ou « *keylogger* » ne sont que des cas particuliers de ce type d'infection où leur fonction est de récupérer certaines données de manière automatique, sans intervention humaine extérieure.

---

[35] Dès qu'un programme recopie son propre code, il y a mécanisme viral : plusieurs copies sont présentes dans le système ce qui les distingue des infections informatiques simples. Cette différenciation s'analyse dans le cadre de la phase d'infection du cycle de vie de programme auto-reproducteur (cf. I/A/3).

[36] Ses effets peuvent être aussi variés qu'une consommation excessive des ressources du système hôte, une destruction rapide du plus grand nombre de fichiers possible, une destruction plus discrète et sporadique d'un unique fichier afin de rester invisible le plus longtemps possible, une atteinte à la sécurité du système hôte (mise en place de droits d'accès laxistes, transmission du fichier des mots de passe vers une adresse Internet, etc.…), une participation de la machine à des opérations de terrorisme informatique tels que les *Distributed Denial of Service (déni de service par saturation)*.

[37] Au titre d'un simple rappel mythologique et mythique, les assaillants grecs menés par Agamemmnon, le roi de Mycènes, avaient abandonné sur le champ de bataille, en tant qu'offrande destinée aux dieux, une statue de bois représentant un immense cheval. Ce dernier fut ramené par les troupes troyennes à l'intérieur des murs d'enceinte de la ville sans qu'elles s'aperçoivent qu'il recelait dans ses flancs un véritable commando qui profita de la nuit pour ouvrir les portes de la ville et offrir cette dernière aux soldats grecs.

- Les accès dissimulés

Les accès dissimulés (ou « *backdoors* ») permettent à un utilisateur externe de prendre le contrôle d'une application par des moyens détournés[38]. Ils peuvent être rapprochés des chevaux de Troie, mais ils ne sont toutefois pas identiques. Un accès dissimulé permet à un utilisateur informé, souvent le concepteur du logiciel ou celui qui l'a « amélioré », d'effectuer une action secrète sur un logiciel, afin d'en obtenir un comportement différent. Ainsi, par exemple, via un accès dissimulé, il est possible d'avoir accès à des informations ou des ressources normalement inaccessibles (données personnelles, profil avancé d'utilisateur, courriers électroniques…). Le fait de laisser une porte ouverte dans un logiciel pour pouvoir l'utiliser sans passer par une quelconque phase d'authentification est souvent dû à des programmeurs désirant faciliter la phase de programmation du logiciel[39]. Il s'agit parfois d'accès officiels disposant de mots de passe mais dont la présence n'est documentée que de manière succincte et conduit les maîtres du système, souvent par ignorance, à les laisser en place[40]. Nous noterons au passage que ces infections ne s'ajoutent pas au programme mais qu'elles en font partie intégrante, qu'elles ne sont, en fait, qu'une fonctionnalité supplémentaire et occulte d'un programme.

- Les logiciels espions

Le cas des programmes espions (ou « *spyware* ») se trouve légèrement en marge des infections informatiques car il ne s'agit pas à proprement parler de mécanismes infectieux dans le sens où il s'agit de programmes fonctionnant de manière autonome[41] ou de sous-programmes (les fameux *cookies*, *applet Jav*a et contrôles *ActiveX*) conçus dans le but de collecter des données et de les envoyer à leur concepteur ou à un tiers sans avoir reçu le consentement de l'utilisateur.

Il s'agit cependant de codes malicieux s'incluant dans un système et présentant un risque supérieur à la simple atteinte à la vie privée puisque pouvant provoquer une saturation des systèmes. Et pourtant, il s'agit de programmes largement utilisés par l'industrie informatique dans les buts de renseigner l'éditeur sur l'environnement matériel où il a été installé, les habitudes informatiques de l'utilisateur ou d'autres finalités moins avouables (espionnage industriel, recherche des cyberdélinquants…)

- Autres agents malveillants

Afin de terminer ce rapide panorama des infections informatiques simples, citons, en marge de celles précédemment énumérées, les canulars informatiques (ou « *hoax* »), entreprise de désinformation qui incite l'utilisateur en utilisant de simples techniques d'ingénierie sociale à

[38] On se souvient du premier film du genre « *Wargame* » dans lequel une multitude d'accès cachés permettait de converser avec le noyau d'un système d'information militaire. Plus ancré dans la réalité, Ken Thompson, dans "*Reflections on Trusting Trust*" [Voir 8] décrit un tel mécanisme mis en place sur l'ensemble des systèmes *Unix*.
[39] Et plus particulièrement lors de la phase de débogage du logiciel alors même que le logiciel professionnel est installé sur le site du client.
[40] Nous nous référons ici à l'affaire opposant l'animateur du site *Kitetoa* à la société *Tati* pour l'intrusion du premier dans le système d'information de cette dernière : TGI Paris, 13 février 2002 et CA Paris, 30 octobre 2002.
[41] Par exemple, dans les logiciels *Netscape Communicator* (*SmartUpdate*) de *Netscape* et *Real Jukebox* et *Real Network*, découverts en 1999.

produire des effets équivalents aux virus et aux vers, tant au niveau de la propagation que de la capacité offensive[42], ou alors les bombes ANSI, séquence d'instructions incluses dans un texte qui reprogramme les fonctionnalités associées au clavier.

Bien qu'il y ait une sorte d'auto-reproduction, elle n'est que de nature sociale et non technique, comme en matière de virus ou de vers, et n'a donc pour nous sa place que dans les infections simples, sa propagation étant due uniquement à une action humaine, sans corollaire technique.

b. Les infections auto-reproductrices

D'une manière générale, l'ensemble des programmes auto-reproducteurs dispose d'une structure semblable au sein de laquelle quatre modules sont associés pour son bon fonctionnement : un module de recherche des programmes-cibles, un module de copie, un module d'anti-détection, ainsi qu'éventuellement un module « fonctionnel », lui-même associé quelques fois à un mécanisme de déclenchement différé.

Comme leur nom l'indique, leur finalité est de se dupliquer, afin de se diffuser, de se propager, via les vecteurs pour lesquels ils ont été programmés.

Avant toute autre chose, précisons, encore une fois, que la distinction virus/vers qui va être réalisée est de plus en plus contestée, de plus en plus de codes viraux étant classés par certains dans les virus ou les vers et par d'autres dans l'autre catégorie, dans les deux, voire incluant des infections simples en raison de la complexité croissante des matériaux viraux et du caractère non probant de cette distinction[43].

- Les virus

Comme déjà énoncé, il s'agit d'un code installé au sein d'un programme hôte, capable de se répliquer afin d'infecter d'autres hôtes. Il s'agit donc d'un code qui sera exécuté en supplément lors du lancement d'un fichier qui recherchera des éléments spécifiques non encore infectés et s'y copiera. Si le principe de la réplication multiple d'un code n'a pas, en principe, d'autres répercussions qu'une utilisation minimale des ressources du système, les virus sont de plus en plus souvent employés comme diffuseur pour d'autres entités plus directement malveillantes, telles que celles vues précédemment.

Il existe presque autant de manières de classer les virus que de virus eux-mêmes. Nous allons nous attacher à cette classification en se fondant sur une analyse fonctionnelle de ces virus. Nous noterons au passage que nombre de virus sont dits « variants » c'est-à-dire qu'il s'agit de virus

[42] Par exemple : fausses alertes de virus enjoignant la destruction de certains fichiers, chaînes de solidarité, message enjoignant sa diffusion au plus grand nombre. On remarque, à ce propos, que la plupart de ces « *hoax* » peut être analysée comme du « *spam* » ou courrier non sollicité, et que d'autre part, ils contribuent à la convergence manifeste et actuelle des différents instruments de la criminalité informatique (cf. l'émergence récente du « *phishing* »).

[43] Pour illustrer ces propos, nous citerons le programme Nimda perçu comme un virus, un ver et un cheval de Troie à la fois.

ayant été réécrits par d'autres que l'auteur initial afin d'en modifier le comportement ou de les rendre temporairement indétectés.

Les *virus-système* ont été les premiers virus connus. Ils interviennent avant le lancement du système d'exploitation et des logiciels antivirus et ont par conséquent accès à toutes les données, nonobstant les éventuels droits du système. Ils sont aussi nommés virus dits de « *boot* » ou de secteur d'amorce (ou « MBR » : *Master Boot Record*). Leur mode d'action leur permet d'infecter directement le secteur de démarrage de 512 octets des périphériques physiques ou logiques, accessible en écriture et dont la fonction est de lancer le système d'exploitation, soit en remplaçant le secteur sain par un secteur infecté, soit en faisant appel à des secteurs externes généralement dissimulés ou chiffrés.

Les virus de document, plus connus sous le nom de macro-virus, sont apparus par la suite, en 1995, avec le *virus Concept*. Il s'agit d'un *« code viral contenu dans un fichier de données, non exécutable, activé par un interpréteur contenu de façon native dans l'application associée au format de ce fichier* »[44] ; chaque format de fichier présentant un risque différent pour l'utilisateur en fonction des possibilités ou des failles permettant d'y inclure un code viral. Ils affectent les applications de la suite bureautique *Office* de *Microsoft* presque dans leur globalité. Lors de l'ouverture du document infecté, le code viral se copie dans certains fichiers de modèles qui sont associés au document et accède au système d'exploitation ; ainsi, toute création ou lecture d'un document sain va aboutir à son infection par duplication du code viral dans le document.

Les virus d'exécutables, ou virus programme, infectent une cible binaire à partir d'un fichier binaire déjà infecté et sont donc fortement spécifiques à un format d'exécutables (*.com, *.exe, *.drv, *.vxd, PE et ELF) déterminé à l'avance. Parmi ceux-ci, certains, qualifiés à tort de *virus de Bios*[45], disposent en tant que module pénalisant d'une fonction de réécriture au niveau du Bios.

Parmi ces virus de programme, peuvent être trouvés, en premier lieu, les virus résidents, qui, une fois exécutés, restent actifs dans la mémoire du système et peuvent donc intervenir à tout moment[46]. En outre, il existe des virus dits « blindés » ou « défensifs » qui peuvent inclure des fonctionnalités avancées visant à rendre le traçage, le désassemblage et la compréhension de son code plus difficile et donc allonger la durée des périodes d'infection et d'incubation, des rétrovirus (ou « virus flibustier ») utilisant les points faibles des antivirus (modification des signatures, par exemple) afin de les leurrer et, par conséquent, les rendre inopérants ou encore des virus multipartite comme le virus *Tequila* qui est à la fois un virus-système et un virus de programme.

Citons encore les cas des virus multipartites et des virus combinés. Les premiers sont des virus capables de d'agir sur plusieurs cibles différentes (fichiers, zones-sytème…) comme le virus

---

[44] E. Filiol, op. cit. *supra* p. 117

[45] *Basic Input/Output System* : logiciel de base intervenant juste après le démarrage de l'ordinateur dans le but de tester l'environnement matériel. Les seuls virus connus de ce type (CIH), du fait de la spécificité des matériels, ne font que remplacer le code par le leur : cf. les virus par recouvrement de code traités ultérieurement.

[46] Parmi ceux-ci, on trouve la sous-distinction des virus lents (qui n'infectent que les fichiers exécutables créés ou modifiés) et les virus rapides (qui infectent les fichiers exécutés ou ouverts, par exemple pendant le traitement d'un logiciel antivirus).

Tequila qui peut à la fois être qualifié de virus-système et de virus de programme. Les seconds sont en fait un ensemble de deux éléments viraux, chacun ayant une action virale (infection et charge finale) partielle et anodine[47]. Le virus n'est véritablement efficace que lors de la rencontre de ces deux programmes. Le virus combiné libère alors la totalité de sa charge finale.

A ce niveau, il convient de préciser que certains virus peuvent infecter plusieurs types de cibles appartenant à des systèmes d'exploitation différents. Ces virus multi-plates-formes (ex : *CrazyEddie* ou W32/*Etap.D*) et multi-formats (*Winux/Lindose*) sont complexes à concevoir (infiniment plus que ceux issus des générateurs de virus) et sont encore très peu nombreux.

- Les vers

Très succinctement, les vers[48] (ou « *worms* ») peuvent être définis comme des virus de réseau ; ils profitent, en effet, des fonctionnalités des réseaux informatiques pour se propager et apparaissent ainsi comme une sous-catégorie des virus plutôt que comme une catégorie à part entière[49]. Ils infectent un réseau et non plus un simple ordinateur : ils ne sont de plus présents qu'en un seul exemplaire sur le système. Dès lors, un système devient, vis-à-vis d'un ver, assimilable aux documents ou aux programmes pour un virus : l'infection se situe à un niveau plus élevé du système d'information que pour un simple virus. Les vers sont cependant issus du même principe que les virus. Selon Peter J. Denning[50], un ver est « *un programme capable de fonctionner de manière indépendante, pouvant se propager en exportant une version fonctionnelle et complète de lui-même vers d'autres machines* ». Comme les virus, ils peuvent également être le vecteur d'un autre programme infectieux. Cependant, leur différence réside dans le fait qu'ils ne nécessitent pas d'être attachés à un programme hôte : ils sont autonomes. Ils utilisent les possibilités offertes par les réseaux, généralement le courrier électronique, pour se propager. Leur pouvoir infectieux est donc beaucoup plus important, pouvant faire le tour du monde en quelques minutes[51], tandis que les virus restent cantonnés à une région particulière[52].

Les « vrais » vers sont relativement rares, du fait de la complexité de leur réalisation. Il ne faut pas les confondre avec un autre type de menace, très courante : les virus qui se transmettent par pièce attachée des courriers électroniques à la manière du très connu "*ILoveYou*". De conception beaucoup plus simple, ils demandent une action effective et nécessaire de la part de l'utilisateur pour être devenir actif.

---

[47] Deux modes d'action sont à envisager : le premier virus peut activer le second ou au contraire, les deux virus sont activés indépendamment et doivent donc, par conséquent, être, en même temps, résidents.

[48] Le terme de ver est dû à l'auteur de science fiction, John Brunner, qui, en 1975, dans « *The Shockwave Ride* » développe la notion d"une couleuvre informatique toute puissante ("*tapeworm*").

[49] En effet, admettre cette distinction revient à faire des réseaux un vecteur spécifique d'infection alors que cela n'est pas nécessaire.

[50] Peter J. Denning ,"The Internet Worm" (1989) [Voir 9].

[51] A titre informatif, le ver *CodeRed* V.2 (2001) a infecté, suivant une courbe exponentielle, en 14 heures, environ 360 000 serveurs dans le monde, avec un doublement toutes les 37 minutes ; le ver *Saphirre/Slammer* infectant, en 2003, environ 75 000 systèmes en moins de 10 minutes, avec un doublement toutes les 8.5 secondes. *Brain*, quant à lui a mis un an à quitter le Pakistan pour les Etats-Unis.

[52] Le virus est sensé se propager en se copiant sur différents supports accessibles d'un seul système, la propagation via les réseaux étant alors du ressort des utilisateurs eux-mêmes qui vont transférer les supports infectés soit matériellement soit via les réseaux.

Créés initialement pour réguler le trafic aérien[53], les premiers vers, les vers simples, sont donc d'un niveau technique relativement élevé : ils exploitent les failles de sécurité des logiciels proposant des services réseau, permettant ainsi de forcer l'exécution d'une copie d'eux-mêmes sur une machine distante[54].

Les macro-vers, classés parmi les vers, quant à eux, sont plutôt des programmes hybrides[55], à la fois ver, en tant qu'utilisateur du réseau pour sa transmission, et virus, car ayant besoin d'infecter un support pour se transmettre. De plus, leur activation requiert une action humaine, ce qui correspond plus à un mécanisme de type viral que de type vermiforme. En effet, la dissémination se fait par l'ouverture de pièces jointes contenant des documents infectés et l'envoi de courriers électroniques dont les destinataires sont issus du carnet d'adresse de l'utilisateur-cible usurpant son identité afin d'inciter le destinataire à une certaine confiance et, au final, à l'ouverture de la pièce infectée.

Utilisant aussi le système de la pièce jointe comme vecteur de propagation, les vers de courriers électroniques (ou « *mass-mailing worm* ») sont eux aussi soumis à la classification controversée de vers. A la seule différence des macro-vers, la pièce jointe contient directement le code malicieux, activé directement par l'utilisateur[56] ou indirectement par son logiciel de courrier électronique, en vertu de failles de sécurité[57].

Enfin, troisième catégorie de vers, ces derniers peuvent se propager au travers des réseaux *peer-to-peer* ou encore via les logiciels de messagerie instantanée.

3. Fonctionnement des programmes auto-reproducteurs

Le fonctionnement de ces programmes auto-reproducteurs sera appréhendé tout d'abord au travers des étapes de sa vie artificielle (a), puis de leur mode d'action (b) et enfin par rapport aux fonctionnalités dont ils peuvent être dotés (c).

a. Cycle de vie d'un virus ou d'un vers

En dehors de la période de conception, le cycle vital d'un virus ou d'un ver respecte trois phases identifiables[58]. Ainsi, pendant la phase d'infection, le programme viral va commencer à se

[53] Il s'agit du ver *Creeper/Reaper* (1971). Il signalait aux contrôleurs le moment où le contrôle d'un avion, sur Arpanet, quittait un ordinateur pour être pris en charge par un autre.
[54] L'archétype en est l'"*Internet Worm*" *(1988) : cf. supra (Introduction)*
[55] Ce qui démontre le caractère superficiel de la classification virus/vers, la limite entre ces catégories n'étant pas clairement définie.
[56] Généralement, sous *Windows OS*, ce code se présente sous la forme d'un fichier disposant d'une extension peu connue ou oubliée (*.pif, *.bat, …).
[57] Par exemple, le lancement d'une page au format HTA (dérivation du format HTML) peut lancer une application tierce inconnue. Or certains clients mail sont réglés par défaut, pour lire les courriers avec un format web et activer par conséquent l'application non autorisée.
[58] Mark Ludwig, « *Naissance d'un virus* » (1994), distingue quant à lui sept phases distinctes : création, gestation, duplication, activation, découverte, assimilation et éradication. Pour nous, cependant, ces trois dernières ne font pas partie du rythme vital du virus.

propager dans l'environnement informatique cible, soit de manière passive, suite à la copie et l'exécution du virus dans ce même environnement par l'utilisateur lui-même, soit de manière active par l'exécution du « *dropper* » ou d'un fichier déjà infecté.

Cette phase est suivie de celle d'incubation, la plus longue, exception faite des virus espions qui se désactivent d'eux-mêmes une fois leur fonction réalisée afin que sa présence demeure inconnue (par exemple, le virus *Ymun*). Cette phase va assurer la survie du virus à travers l'ensemble de ses copies dans l'environnement cible et va permettre d'empêcher ou, à tout le moins, éviter sa détection par l'utilisateur ou par un antivirus, par l'application de techniques particulières, ou simplement en évitant les erreurs d'exécution et message d'alerte du système.

Le cycle se termine avec la phase de « maladie » et le lancement de la charge finale, plus ou moins néfaste, du virus ou du ver. Elle peut ainsi être de nature « non létale » et provoquer, par exemple, l'affichage d'images ou l'émission d'un message, ou de nature « létale » et porter atteinte aux cinq principes de la sécurité informatique que sont la disponibilité, la confidentialité, l'intégrité, la non-répudiation et l'authenticité des données.

Il convient de préciser à ce stade de l'analyse que le moindre dysfonctionnement d'un quelconque outil informatique n'est pas naturellement dû à la charge finale d'un virus. Si nous restons dans notre domaine d'étude, ils peuvent être tout aussi bien dus au principe de fonctionnement du virus, comme nous le verrons plus loin (cf. II/A/4), ou avoir une toute autre cause. Notons ainsi que les virus ne détruisent pas le matériel lui-même mais seulement les éléments logiciels qui y sont intégrés[59].

b. Mode d'action des virus et des vers

Afin de comprendre la manière dont on peut les appréhender, il est nécessaire de comprendre les modes selon lesquels les virus peuvent se dupliquer. Ainsi, on s'aperçoit qu'ils peuvent agir, tant au niveau de l'exécutable compilé, qu'au niveau du code source.

S'agissant du premier cas, il existe plusieurs techniques. Le virus peut, en effet, agir par recouvrement de code (le code viral substitue une partie de l'en-tête ou du code du programme cible par le sien propre[60]), par adjonction de code (il remplace l'en-tête du programme par la sienne et se place à la suite du programme), par entrelacement de code (il se loge dans des zones allouées au fichier mais non utilisées[61]) ou encore par accompagnement de code (il ne s'insère pas dans le programme cible mais crée un fichier supplémentaire qui va accompagner la cible ;

[59] C'est notamment le cas du virus CIH qui altérait le Bios de la carte mère des systèmes, provoquant son remplacement plus par facilité que par véritable endommagement. On peut toutefois soulever le problème d'hypothétiques virus modifiant les données substantielles des systèmes (tensions, fréquence, …) qui pourraient provoquer leur indisponibilité de manière rapide. On ajoutera que dans ce cas, ils seraient extrêmement spécifiques car ils ne pourraient altérer qu'un nombre limité de matériel … et donc, par-là, ils sont presque indétectables.

[60] A noter que certains considèrent la sous-distinction du virus « cavité », virus avec recouvrement de code mais conservant l'information en ne se copiant que dans une zone constituée entièrement de zéro.

[61] Ce mode est relativement limité puisque exploitant un seul format d'exécutable : le format *Portable Executable* des exécutables 32 bits des systèmes d'exploitation *Windows*.

lors de l'exécution du programme, la copie virale contenue dans ce fichier est lancée en premier, permettant au virus de se propager, puis le programme légitime est lancé).

Ces diverses techniques ont divers avantages ou inconvénients en terme de furtivité et de respect du programme hôte, rendant ainsi leur détection plus ou moins facile.

Les virus en code source[62], quant à eux, constituent une catégorie à part. Ainsi, le programme infectieux, sous forme exécutable, se copie, mais contrairement aux modes d'actions vus précédemment, il va s'intégrer dans le code source du programme cible, lequel doit alors être compilé pour produire un exécutable valide. La simple duplication ne suffit donc pas. L'intérêt de ce type de virus est, d'une part, de produire, après compilation, un exécutable présentant une parfaite homogénéité, contrairement aux autres modes d'infection où le code binaire est modifié ultérieurement et, d'autre part, de contourner plus efficacement les protections antivirales[63].

c. Techniques avancées

Afin de contrer les mécanismes qui pourraient empêcher leur propagation, essentiellement les logiciels antivirus, les infections informatiques ont été pourvues de techniques avancées visant à leur permettre une survie accrue en milieu « hostile ».

Une des techniques les plus utilisées est celle de la « furtivité ». Elle consiste elle-même en un ensemble de procédés visant à leurrer l'utilisateur, le système et les logiciels de protection afin de faire croire à l'absence du code viral dans le système.

Enfin, le code peut être chiffré, chaque copie du virus pouvant se différencier des précédentes et donc éviter la reconnaissance du virus par le système de recherches de signatures virales des logiciels antivirus[64]. Par ailleurs, nous noterons qu'il existe plusieurs niveaux de chiffrement/cryptage avec, en premier lieu, un cryptage d'une partie du virus avec une clé différente à chaque fois (excepté le décrypteur), en second lieu, un mécanisme permettant de modifier le décrypteur à chaque infection et, en dernier lieu, une modification de l'ensemble du moteur de chiffrement à chaque infection procédé qui est alors appelé polymorphie[65].

Les principaux concepts de la technologie virale étant précisés, analysons la façon dont le droit appréhende l'ensemble de ces organismes infectieux d'une manière globale (B).

---

[62] (Par exemple, « *Shifting Objectives* » apparu en janvier 1984)

[63] On ajoutera les avantages dus à tout programme en code source c'est-à-dire, notamment, les capacités d'adaptation à différents systèmes d'exploitation. Eric Filiol, op. cit. *supra* p. 106, ajoute que la possibilité d'un code d'intégrité (par exemple, une fonction de hachage MD5) affecte peu de tels programmes, car il peut tout à fait être substitué.

[64] Le polymorphisme peut s'acquérir soit par réécriture du code par un code équivalent soit par l'utilisation de techniques de chiffrement basique sur tout ou partie du virus ou du ver. Certains techniciens vont être plus précis encore et ajouter à ces techniques, les virus dotés d'algorithmes génétiques (dérivés des virus polymorphes, ils « connaissent » leur nature et ne vont produire que des formes posant des problèmes aux logiciels antivirus qu'ils vont rencontrer) ou les virus répressifs (qui vont attaquer le logiciel antivirus, voir, le transformer en un cheval de Troie).

[65] La FAQ *alt.comp.virus* parle d'un « *Mutation Engine* », module qui pourrait rendre polymorphe n'importe quel virus par l'adjonction de générateurs de nombres aléatoires.

Section B - Analyse juridique classique de la cybercriminalité sous l'angle viral

Les virus peuvent être appréhendés pénalement de diverses manières. Nous analyserons tout d'abord les infractions traditionnelles (1), puis les infractions spécifiques de la loi dite « Godfrain » (2), les modifications effectuées par la loi pour la Confiance dans l'Economie Numérique (3), la loi « Informatique et libertés » (4) et enfin nous sortirons du champ du droit français pour observer certaines des initiatives nationales et supranationales (5). Il convient cependant de préciser qu'en matière de virus, le caractère international de l'infraction sera souvent probant.

Ainsi, s'agissant d'un délit ou d'un quasi-délit, les articles 5§3 de la Convention de Bruxelles et du règlement 44/2001, posent une règle de compétence spéciale en faveur du tribunal où le fait dommageable s'est produit ou risque de se produire. Ce lieu peut être aussi bien celui où le dommage est survenu que celui de l'événement causal qui est à l'origine de ce dommage[66]. Les tribunaux français seront donc compétents de manière très fréquente, le problème résiduel étant la condamnation d'une personne à l'étranger. A titre informatif, rappelons que l'auteur du ver « *I Love You* » n'a pu être condamné car à l'époque des faits, il n'existait pas aux Philippines de texte incriminant la création et la diffusion de virus. Nous pouvons dès lors soulever la question des paradis numériques et du devenir de la répression quand l'auteur d'un virus demeure ou héberge son virus dans ces pays là.

1. Les prescriptions traditionnelles et les virus

Il s'agit principalement d'étudier certaines des dispositions du Livre III du Code Pénal « Des crimes et délits contre les biens » et notamment l'escroquerie (a), l'abus de confiance (b) et le vol (c). En effet, il est maintenant communément admis que les infractions traditionnelles atteignant les biens ne trouvent pas d'exceptions dans le domaine informatique. Même si ce secteur n'était pas connu originellement du droit pénal, son applicabilité ne fait aucun doute et une escroquerie réalisée à l'aide d'un ordinateur reste avant tout une escroquerie.

Sans s'attarder sur la qualification des éléments nécessaires à la constitution de l'infraction, nous allons directement nous intéresser aux relations que pourraient avoir les mécanismes infectieux avec ces infractions et notamment au travers de la question de leur application aux biens immatériels. Les programmes viraux entrent précisément dans le champ de cette application, leur activation ayant des implications logiques sur des éléments immatériels, que cela soit en terme de données ou en terme de disponibilité d'un système.

a. L'escroquerie

L'escroquerie est la remise volontaire de la chose suite à des manœuvres d'origine frauduleuse. En la matière, il est admis, depuis la réforme du Code Pénal du 1er janvier 1994, qu'elle puisse avoir pour objet une prestation de service et donc, par conséquent, une chose immatérielle. On pourrait donc admettre l'application de l'escroquerie à des manœuvres frauduleuses utilisant un programme infectieux pour se faire remettre, par l'action de l'utilisateur, une donnée ou pour

[66] CJCE, 30 novembre 1976, aff. C-21/76, *Mines de potasse d'Alsace* : Rec. CJCE, p. 1735

accéder à des informations (cheval de Troie, accès dissimulé, programme espion) permettant de faciliter ou de provoquer cette remise de la chose[67]. D'une manière plus générale, on peut admettre que l'abus des possibilités d'un système pour se faire remettre une donnée ou une prestation[68] rentre dans le champ de l'article L. 313-1 du Code Pénal. Dès lors, l'auteur d'un programme viral exploitant simplement une faille d'un système pourrait être sanctionné de ce chef, si tant est que les éléments matériel et moral de l'infraction soient constitués. Les mécanismes viraux ne peuvent donc être appréhendés que de manière accessoire via cette disposition.

b. L'abus de confiance

En matière d'abus de confiance, c'est-à-dire en matière de détournement d'une chose remise volontairement, les biens immatériels sont exclus de cette prescription de manière classique[69]. Cependant, l'évolution de la jurisprudence s'est infléchie et elle a, peu à peu, reçu ces biens immatériels dans le champ de l'article L. 314-1 du Code Pénal et a admis, en premier lieu, les valeurs mobilières au titre d'un écrit constitué par l'inscription en compte[70], puis un numéro de carte bancaire, retenant que les « dispositions de l'article 314-1 s'appliquent à un bien quelconque et pas seulement à un bien corporel »[71]. Toutefois, en dehors des hypothèses marginales ou une donnée a été confiée à un tiers et que celle-ci se trouve détruite par un organisme informatique viral, nous voyons mal les interactions qui pourraient exister entre l'abus de confiance et ces derniers. La question du vol est plus intéressante.

c. Le vol

Les articles L. 311-1 et suivants du Code Pénal qui disposent du vol, à savoir la soustraction frauduleuse de la chose d'autrui, sont susceptibles d'appréhender les biens immatériels dans la mesure où le Code Pénal considère comme tel la soustraction frauduleuse d'énergie. Toutefois, le texte de l'article L. 311-2 énonce que celle-ci est assimilée au vol et donc qu'il ne s'agit pas exactement de vol. En effet, s'agissant d'informations ou de données, cibles privilégiées des mécanismes viraux malicieux, la solution est toute autre.

Le droit pénal appréhende correctement le vol d'information à travers le vol de son support, qu'il s'agisse d'une soustraction de la chose permanente ou qu'il s'agisse d'une appréhension frauduleuse pendant le temps nécessaire à la reproduction de l'information[72], mais le vol

---

[67] CA Aix-en-Provence, 13 septembre 1972 ; *JCP 1972 II. 17240, note A.C.* précise que peu importe que les manœuvres frauduleuses se soient exercées directement sur l'esprit d'une personne ou se soient réalisées via des manipulations destinées à fausser le fonctionnement normal d'un appareil automatique.

[68] Arrêt précité (*supra. n°64*) et CA Douai 16 juin 1972, *Gaz. Pal. 1972 2.722*

[69] Cass. Crim. 9 mars 1987 ; *Bul.l Crim. N°111 ; JCP 1988 II 20913, note Devèze ; Rev. Sc. Crim. 1988 311, obs. Bouzat.* retient que l'abus de confiance ne peut porter que sur l'écrit constatant le contrat mais non sur les stipulations qui en constitue la substance.

[70] Cass. Crim 30 mai 1996*, Bull. Crim. 1996, n° 224, p. 625.*

[71] Cass. Crim. 14 novembre 2000*, Bull. Crim. 2000, n°342, p. 1014.*

[72] Cass. Crim. « Logabax », 8 janvier 1979 *; Bull. Crim. N°13 ; Dalloz 1979. 509, note Corlay et IR. 182, obs. Roujou de Boubée ; Gaz. Pal. 1979.2.501 ; Rev. Sc. Crim. 1979.571, obs. Bouzat.*

d'information, lui, est encore inconnu car, si des arrêts ont pu laisser penser le contraire[73], le vol ne s'applique qu'à une chose « *matérielle susceptible d'appréhension [physique] par l'auteur du vol »* et le « vol d'information » ne peut être appréhendé par la loi pénale qu'à travers le vol de son support matériel. »[74]. Par conséquent, ni le « vol » de temps machine, ni le « vol » de bande passante ne peut être appréhendé par cette disposition.

A tout le moins peut-on ajouter que les mécanismes viraux peuvent être appréhendés par les textes sur la protection de la vie privée ou par ceux sur la protection du secret des correspondances privées[75] mais aussi, par ceux relatifs à la contrefaçon des logiciels, telle que la loi du 3 juillet 1985 sur la protection des logiciels par le droit d'auteur ou encore par des textes très spécifiques tels que ceux régissant l'atteinte aux intérêts fondamentaux de la nation (article L. 410-1 et suivants du Code Pénal). Toutefois, cela ne couvre, comme les infractions précédentes, que des hypothèses marginales où les organismes informatiques viraux ne sont appréciés qu'eu égard à l'un de leur effet particulier et ne font pas l'objet d'une appréhension globale, comme lors de la réforme de 1988[76].

2. La loi du 5 janvier 1988 « Godfrain »

La loi dite « Godfrain » du 5 janvier 1988 qui fixe un nouveau cadre législatif en introduisant sept nouveaux articles dans le Code Pénal, apparaît dans un contexte mouvementé[77], alors que le système d'information n'était protégé que de manière accessoire par quelques rares textes, comme la loi « Informatique et libertés », du 6 janvier 1978, ou la loi du 3 juillet 1985 précitée. Aucune répression pénale spécifique et globale ne permettait d'appréhender véritablement une intrusion virale, volontaire ou non, dans un système à quelque fin qu'elle soit. La volonté de mettre en œuvre une répression globale, incluant les mécanismes viraux conduit, à l'adoption de la loi du 5 janvier 1988 qui ajoutait au code pénal un chapitre « *Des atteintes aux Systèmes de Traitement Automatisé de Données* ». Sanctionnant à la fois des actes dirigés contre le système informatique et des actes commis à l'aide de l'outil informatique, nous observerons toutefois, préalablement, que ces articles n'ont pas pour effet d'établir une appropriation des informations prises en tant que telles.

---

[73] Arrêt précité ainsi que Cass. Crim. 12 janvier 1989, *Bull. Crim. n°14* et Cass. Crim. « Antonioli », 1er mars 1989, Bull. Crim., 1989, n°100 ; Droit de l'informatique, 1990, p.38, note J.Huet.

[74] CA Grenoble, 4 mai 2000.

[75] Loi du 10 juillet 1991 relative au secret des correspondances émises par voie de télécommunications.

[76] Nous pourrions ajouter que les virus peuvent être appréhendés aussi par d'autres textes relatifs au faux (art. 441du Code Pénal), à l'atteinte aux intérêts fondamentaux de la nation (art. 410-1 et suivants du Code Pénal) mais leur mise en œuvre demeure de nature résiduelle.

[77] Alors que le CCC (*Chaos Computer Club*) en Allemagne ou le CLODO (*Comité Liquidant Ou Détournant Les Ordinateurs*) en France faisaient parler d'eux dans certains cercles fermés (espionnage industriel, pénétration de systèmes militaires, …), étaient publiés, le 28 novembre 1984, les détails d'une intrusion que des journalistes du « Canard enchaîné » avaient réalisée dans une base de données sensible à l'aide d'un simple minitel, les magazines reprenant le thème quelques années plus tard : « *Détournement à l'ordinateur. L'employé modèle avait escroqué 7 millions de francs à la banque* », le Figaro, 20 mai 1985, « *Comment vous faire ruiner par les pillards de l'informatique* », L'Expansion, 18 décembre 1987.

Afin d'analyser cette loi, il convient de définir la notion de Système de Traitement Automatisé de Données (a) avant d'étudier l'accès et le maintien frauduleux (b) ainsi que les atteintes au système (c) ou aux données (d).

a. La notion de Système de Traitement Automatisé de Données

Bien que cette notion ait aujourd'hui disparue au profit de celle, plus globale, de système d'information, il convient néanmoins de la préciser. Il n'existe cependant pas de définition légale ; le Sénat en avait proposé une[78] mais qui, pour ne pas lier l'incrimination à un état particulier de la technique, n'a pas été conservée.

Les tribunaux ont aujourd'hui de cette notion une conception large, sans considération d'une taille ou d'une capacité de traitement minimale, et admettent en tant que système : le réseau France Télécom, le réseau du GIE *Carte Bancaire*, un disque dur, un radiotéléphone, un ordinateur isolé, un réseau[79]. On peut néanmoins penser que cette notion sera facilement extensible aux nouveaux produits informatiques : réseaux sans fil (*Wifi*, *Bluetooth*, …), assistants numériques personnels, baladeurs, montres, etc[80]. Nous noterons d'ores et déjà que c'est le système, en tant que nouvelle universalité de fait, qui fait l'objet de la protection et non les éléments qui composent cet ensemble[81], que ce système soit achevé ou non[82]. Il ressort de cette conception que les unités de traitement de l'information sont couvertes par cette notion mais aussi l'ensemble de leurs périphériques et des réseaux électroniques auxquels elles sont reliées. Nous observerons toutefois que dans l'esprit de la notion de système correspondait initialement à la notion d'ordinateur, qu'ils soient reliés ou non[83]. Aujourd'hui, nous pouvons dire qu'il y a STAD (Système de Traitement Automatisé de Données) dès lors que nous sommes en présence d'une machine de Türing, de la mise en œuvre d'une problématique de flux concernant des données. Un simple support de données ne sera donc pas considéré comme un STAD.

Par ailleurs, se pose la question de la nécessité ou de l'indifférence de la présence dispositifs de sécurité pour la constitution de l'infraction. La jurisprudence apporte à ce propos une réponse négative et ne retient pas l'existence d'un dispositif de sécurité en tant que condition préalable à la réalisation de l'infraction[84]. Cette question peut être appréciée au regard de l'élément intentionnel, le bris d'une protection caractérisant l'intention de nuire de l'auteur. En l'absence de dispositif de sécurité, il sera effectivement plus difficile de prouver cet élément.

---

[78] Le Sénat désirait définir un STAD comme « *tout ensemble composé d'une ou plusieurs unités de traitement automatisées, de mémoires, de logiciels, de données, d'organes d'entrées-sorties et de liaison qui concourent à un résultat déterminé, cet ensemble étant protégé par des dispositifs de sécurité* » (Rapport J. Thyraud Doc. Sénat 1987-88 n°3 p52 [Voir 10]).

[79] CA Douai, 7 oct. 1992 pour le disque dur; CA Paris, 18 nov. 1992 pour le radiotéléphone et Trib. Corr. Paris, 25 fev. 2000 pour le réseau du GIE *Carte Bancaire*.

[80] D'autres éléments nous paraissent toutefois ne pas être inclus dans cette notion : un réseau/pont *bluetooth* qui se créerait ponctuellement entre deux téléphones portables sans que leurs utilisateurs en ait conscience par exemple. L'hypothèse reste toutefois marginale et il semble que cette notion trouve une limite liée à l'utilité même de l'atteinte.

[81] L'arrêt de la cour d'appel de Douai susvisé prône la solution contraire mais reste vivement critiqué.

[82] Cass. Crim. 5 janvier 1994 : Gaz. Pal. 1996 2 p. 419 note Catherine Latry-Bonnart.

[83] Voir Rapport J.Thyraud, op. cit. supra note 75.

[84] CA Paris, 5 avril 1994 ; Dalloz 1994 IR 130.

A l'évidence, malgré le fait que l'information soit de libre parcours, via la notion de STAD, nous nous trouvons en face d'un système de monopolisation de la consultation de l'information[85], monopole qui est protégé à des degrés divers, l'accès étant, comme nous allons le voir, réprimé moins fortement que les véritables atteintes au système ou aux données. Ceci étant précisé, nous allons donc maintenant examiner la loi du 5 janvier 1988 au regard des mécanismes infectieux.

b. L'accès et le maintien frauduleux dans un STAD

Ces infractions résultent de l'article 323-1 du Code Pénal[86], lequel, tout comme ceux qui vont suivre, a été rédigé de manière volontairement large afin de ne pas être lié à des notions trop techniques et donc susceptible de devenir inefficace à court terme.

Ainsi, en premier lieu, est réprimé l'accès à un STAD. Il vise tous les modes de pénétration ou d'intrusion irrégulière dans un système informatique. Etudié à l'aune des mécanismes infectieux, le fait de se brancher sans droits sur un réseau et d'en intercepter le trafic grâce à un programme malveillant simple (un cheval de Troie de type « *sniffer* » ou« *keylogger* » par exemple[87]), un code d'origine viral le véhiculant ou visant l'insertion d'un tel programme (protocole d'administration à distance : *Telnet*, SSH, …) pourrait emporter une telle qualification pénale[88], sans qu'il soit nécessaire de démontrer un quelconque préjudice lié à cet accès.

La notion d'accès est avant tout une notion juridique. Elle peut avoir deux occurrences : la première est dite « active » : un accès intrusif tel que l'exploitation d'une faille logicielle (notamment par débordement de mémoire ou « *buffer overflow* ») ; et la seconde, « passive » : simple interception d'informations émises par le système (analyse du trafic d'un réseau, par exemple) sans émission de données de la part du cyberdélinquant. Bien que, dans ce dernier cas, il n'y ait pas d'accès technique direct dans le système, on considère aujourd'hui qu'il y a bien un accès au sens juridique, accès frauduleux s'il est réalisé sans l'autorisation du maître du système.

Par ailleurs, le simple maintien dans un système est susceptible de constituer l'infraction, et ce, même s'il résulte d'un accès régulier antérieur. Les deux notions sont effectivement incriminées séparément par la loi.

---

[85] Hervé Croze, « *L'apport du droit pénal à la théorie générale de l'informatique (à propos de la loi n°88-19 du 5 janvier 1988 relative à la fraude informatique)* », Semaine Juridique, éd. gale I N°18-3333

[86] Art. L. 323-1 Code Pénal : « *Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30 000 euros d'amende.* » « *Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45 000 euros d'amende.* »

[87] TGI Paris, 16 décembre 1997 ; Gaz. Pal. 1998 2. Somm. 433, note C. Rojinsky.

[88] Dans une acception récente, les techniques actuelles de « *war driving* » (la recherche de réseaux Wifi à la norme 802.11x ouverts) pourraient être sanctionnées sur ce fondement. L'installation de bornes d'accès sans fil permet un accès dans le périmètre dans lequel la borne émet. Il est donc possible à toute personne de s'y connecter. Des dispositifs de sécurité ont été pensés et inclus dans le protocole 802.11x afin de limiter cette liberté d'accès mais, en sus des failles déjà découvertes, ils ne sont pas toujours activés. Nous pouvons donc facilement imaginer un programme viral qui se propage par bornes interposées et son insertion sur un tel réseau.

Dans le cas d'un accès régulier, le maintien devient irrégulier dès lors que son auteur se trouve privé de toute habilitation, par exemple en effectuant une autre opération que celle initialement prévue ou en dépassant le temps de connexion autorisé. Ainsi, le dépôt ou l'activation d'un code malicieux sur un serveur public, à quelque fin que ce soit, pourrait entrer dans le champ du maintien. Nous noterons cependant que l'accès ou le maintien doivent être frauduleux, à savoir qu'ils « *doivent être faits sans droit et en connaissance de cause* »[89] c'est-à-dire que l'acte ne doit pas résulter d'une simple erreur et n'être que volontaire mais que son auteur doit avoir conscience de l'irrégularité de l'acte. A ce propos, nous ajouterons que l'expression « *sans droits* » n'est pas une référence aux droits informatiques tels qu'on les entend généralement en matière d'administration de système. Il n'est pas nécessaire que des comptes administrateurs et utilisateurs soient créés sur le système pour qu'il y ait une intrusion « *sans droits* » ; il suffit que cette intrusion aille à l'encontre de la volonté initiale du maître du système.

Certains éléments sont toutefois indifférents à la qualification de ces infractions. Ainsi, peu importe la présence ou non d'une intention de nuire, le procédé ou le lieu utilisé pour réaliser l'infraction, les actes effectivement effectués, que l'accès ou le maintien concerne tout ou partie du système, qu'il ait été effectué directement ou au travers d'une application complexe. On observera cependant que l'alinéa 2 de l'article 323-1 aggrave la peine en cas d'atteinte aux données lors de l'accès ou du maintien[90]. Cependant, nous pouvons noter que, s'agissant de l'alinéa 2, l'infraction est constituée dès lors que le simple élément matériel est présent : des altérations résultant d'une simple maladresse ou des principes actifs propres au système suffisent.

c. Les atteintes volontaires au fonctionnement du système

Conçu pour réprimer le sabotage informatique, l'article 323-2 du Code Pénal sanctionne aussi bien le fait d'entraver que celui de fausser le système[91] et correspond à la disposition qui réprime traditionnellement les infections informatiques. La notion d'entrave est déjà connue puisque présente en matière de droit social ou de circulation routière. Cependant, une transposition pure et simple aux nouvelles technologies est à éviter. En effet, en matière d'atteinte à un système, elle suppose l'accomplissement d'un acte positif et ne saurait se contenter d'une abstention fautive[92]. En l'espèce, l'entrave réside dans le fait d'empêcher le fonctionnement logiciel ou matériel du système en provoquant une paralysie partielle ou totale, progressive ou instantanée, temporaire ou définitive, ponctuelle ou permanente et enfin simple ou récurrente de celui-ci, ou plus simplement une gêne quelconque[93]. L'étendue de cette disposition permet d'appréhender la plupart des comportements finaux issus des mécanismes viraux et notamment ceux issus des

[89] CA Paris, 5 avril 1994 ; *susvisé*.
[90] Art. L.323-1 al.2 Code Pénal, op. cit. *supra*, note n°46.
[91] Art. L. 323-2 Code Pénal : « *Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende*. »
[92] CA Paris, 1994 ; *susvisé.*
[93] TGI Le Mans 7 novembre 2003 (http://www.juriscom.net/jpt/visu.php?ID=390): cet arrêt a jugé qu'un simple envoi massif de courriers électroniques dénigrants constitue une entrave. Par conséquent, on peut supposer que l'infection d'un système avec un code viral permettant, via un serveur proxy cet envoi massif constitue elle-même une entrave au fonctionnement du système et ce, même si la gêne intervient au niveau du système et non de l'utilisateur.

bombes logiques associées à ces mécanismes en tant que charge finale (consommation excessive de ressources du système, interruption des logiciels d'exploitation ou d'application, saturation du système de fichier, outrepassation de la convention d'utilisation du système …).

De manière opposée, la notion de « *faussement* » ne dispose d'aucune référence antérieure à la loi de 1988 dans le droit français. Il en résulte, eu égard à l'esprit de la loi, une interprétation large de la disposition et l'idée générale qui prédomine est celle d'un comportement du système anormal ou non prévu par le maître du système. Fausser un système serait donc altérer, dénaturer son comportement de manière insidieuse, sournoise, lui faire produire un résultat non attendu[94]. Dès lors, toute activité non désirée d'un programme, sans exceptions, entre dans le champ de cet article[95].

Nous pouvons même nous demander à quel niveau de consentement nous devons nous arrêter pour considérer qu'une activité du système différente de celles prévues constitue un « *faussement* ». Si l'on peut raisonnablement penser qu'un logiciel « autorisé » exécutant une fonction occulte tombe sous le coup de cette disposition, peut-on aboutir à la même solution, à l'extrême, dans le cas d'un même logiciel « autorisé » qui utilise, pour exécuter sa tâche, des fonctionnalités qui ne sont pas directement nécessaires à son accomplissement[96] ? Ne pourrait-on pas analyser ceci en un faussement du système ? En effet, nous pourrions dire que l'utilisateur du logiciel a consenti au fonctionnement du logiciel par rapport à certaines fonctionnalités et non par rapport à des commandes ou des routines logicielles sans rapport avec celles-ci ? Cependant, cela nous semblerait être une interprétation trop extensive de la disposition et une lecture trop restrictive des licences de ces logiciels. Il semble donc qu'il faille considérer le consentement de l'utilisateur à l'aune d'un consentement global des fonctionnalités et des procédés de mise en œuvre de celles-ci, en dehors de toute fonction occulte évidemment.

S'agissant d'atteintes volontaires, il est nécessaire, pour que le délit soit constitué, que l'auteur de l'infraction ait la conscience de l'entrave ou du « *faussement* »[97]. L'intention de nuire n'est pas exigée mais l'auteur doit se comporter en contradiction avec la volonté du maître du système. Nous ajouterons que ce texte est destiné à protéger aussi bien le maître du système que les tiers bénéficiaires des traitements informatiques[98].

d. Les atteintes volontaires aux données

---

[94] Thiébaut Devergranne, *MISC, le journal de la sécurité informatique n°2 (2002)*, ajoute qu'on pourrait appliquer l'article à la pratique du « défacement » c'est-à-dire la modification par une personne non autorisée de la page d'accueil d'un site Internet. Nul doute, à ce propos, qu'un site web serait considéré comme un STAD et qu'on pourrait plaider le « faussement » voire l'entrave, temporaire mais néanmoins réelle, au fonctionnement du système.

[95] Ainsi, un simple économiseur d'écran et, a fortiori, un économiseur qui permettrait de partager les ressources du système (programme SETI, Folding@home…) pourrait être visé par cette infraction.

[96] Nous visons expressément le cas de routines superflues ou oubliées ou de fonctionnalités que l'utilisateur ne peut modifier ou empêcher (notamment accréditation en ligne des fichiers musicaux au format WMA, installation d'une « *backdoors* » de maintenance voire failles de sécurité) et issues d'un processus antérieur ou contemporain au fonctionnement du système.

[97] Cass. Crim., 12 décembre 1996, « *Excelsior informatique* », Comm J. Bertrand, Expertises, mars 1998, p. 70.

[98] Rapport J-J Hyest, Doc. Ass. Nat. 1991 N°2468, p. 113 [Voir 11].

Afin de compléter l'arsenal répressif du juge en matière de code viral, l'article 323-3 du Code Pénal incrimine les atteintes aux données d'une manière autonome[99]. Thiébaut Devergranne[100] fait, à ce propos, judicieusement remarquer que la distinction formelle entre les atteintes au système et les atteintes aux données n'est pas de meilleur aloi, la modification ou la suppression de données pouvant entraver et à tout le moins fausser leur système hôte. Ainsi, cette disposition n'a plus pour but de protéger le système mais les données elles-mêmes. Les caractéristiques du système, la manière dont les données sont accédées ou la régularité de celles-ci, importent donc peu, de même que le bon ou le mauvais fonctionnement du système après l'atteinte aux données.

Afin de mesurer la portée de cette disposition, il est important de connaître l'exacte étendue de la notion de données. Si, par définition, il s'agit d'une chose immatérielle, une donnée n'est cependant ni une simple information, ni une simple série d'instruction. Il s'agirait plus de la représentation d'une information sous une forme conventionnelle destinée à favoriser son traitement. Cette notion de traitement se retrouve en matière de programmation traditionnelle/procédurale dans laquelle les traitements sont séparés des données. Partant de cette définition, une atteinte à un traitement, autrement dit un programme, n'entrerait pas dans le champ de cette définition. Cependant, pour nuancer nos propos, il apparaît aussi que ceci ne serait applicable qu'aux programmes les plus simples, ceux qui sont plus complexes intégrant en tout état de cause des données dans le corps même de leur code[101]. Par ailleurs, l'atteinte à un programme, même simple, suppose, à un moment quelconque, un accès (au minimum, un accès à distance via un outil qui pourra être préconfiguré pour cette atteinte, comme un code viral) et donc une appréhension par l'article L.323-1 du Code Pénal. En tout état de cause, la jurisprudence ne semble aujourd'hui pas retenir la distinction programmes et données.

En outre, nous noterons, élément indifférent eu égard à la constitution de l'infraction, qu'en matière de code malicieux, l'atteinte aux données est perçue comme une conséquence, volontaire ou non, et non comme un préalable à une autre action. Selon nous, cela renforce la portée de la nécessité de l'élément intentionnel. De nombreuses affaires ont été jugées dans le sens de la relaxe de prévenus responsables de l'introduction de codes infectieux sur des supports magnétiques sans qu'ils aient eu connaissance de celle-ci[102].

En tout état de cause, un virus, qui est, sans contestation possible, un programme informatique, est lui-même une donnée. Son ajout à un système d'information, même sans destruction, constitue une altération de l'ensemble de données de ce système. Il nous semble donc qu'un virus, même inactif, constitue une altération des données du système. Au surplus, le virus devient une donnée du système lui-même et son activation du fait de sa programmation par son concepteur constitue une altération du virus et donc, par conséquent, des données du système. Le

---

[99] Art. L. 323-3 Code Pénal : « *Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende*.»

[100] Thiébaut Devergranne, « La loi « Godfrain » à l'épreuve du temps » *MISC, le journal de la sécurité informatique n°5 (2003).*

[101] Il nous semble impossible, en pratique, de créer un code viral doté de la capacité de différencier, à l'intérieur d'un programme, le code correspondant aux unités de traitement de celui des données elles-même.

[102] Cass. Crim. 12 décembre 1996, op. cit. note n° 94.

code viral peut donc être appréhendé sur ce point à plusieurs niveaux de son propre fonctionnement.

Par ailleurs, la loi du 5 janvier 1988 sanctionne l'association de malfaiteur en matière informatique, en visant les clubs de piratage et les clubs des codeurs de programmes infectieux[103] ; étant précisé qu'il y a groupement de malfaiteur dès lors qu'il y a concours de deux volontés ou plus, conscience des infractions et qu'il doit se concrétiser par un ou plusieurs faits matériels[104]. La loi prévoit la répression de la tentative[105], de nombreuses peines complémentaires ainsi que la responsabilité pénale des personnes morales[106]. Toutefois, l'incitation à l'entrave d'un système n'est pas réprimée[107].

Il résulte de ce qui précède que la législation actuelle sanctionne pour la forme, mais pas pour les effets. Cela peut paraître surprenant de disposer de délits formels pour une matière où demeurent de nombreuses inconnues, mais cela a été vu, à l'époque[108], comme la solution qui permettait d'inscrire le texte dans le temps et de respecter le principe de neutralité technique de la loi. L'étude de la jurisprudence ne nous permet, toutes infractions confondues, de recenser qu'une trentaine de décisions prises sur le fondement de la loi du 5 janvier 1988, ce qui, dans le contexte de société de l'information actuel est relativement étrange. Des facteurs sociaux semblent, par conséquent, être intervenus afin de limiter son effet, et notamment en matière de programmes viraux (impossibilité à retrouver l'auteur international du programme, peur de l'annonce publique d'un problème informatique, méconnaissance des risques, …). En effet, on constate que les acteurs de l'informatique sont encore frileux à admettre un incident au sein de leur système d'information. Mais peut-être est-ce la raison de la volonté du législateur d'accroître encore le champ des infractions liées à l'informatique et notamment en matière de programmes viraux ?

3. L'article 46 de la loi pour la Confiance dans l'Economie Numérique du 21 juin 2004

Au terme des nombreux amendements sur cet article du projet de loi, tant celui-ci provoqua des remous dans le milieu des professionnels de la sécurité informatique, le projet de loi pour la Confiance dans l'Economie Numérique fut adopté le 13 mai dernier et entériné par la décision du Conseil Constitutionnel du 10 juin. Toutefois, l'article et la loi, promulguée le 21 juin, restent vivement critiqués. En effet, en plus de permettre la saisie des données informatiques nécessaires à la manifestation de la vérité (article 41 et suivants) et d'augmenter la durée des peines

---

[103] Art. L. 323-4 Code Pénal : « *La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée*. »

[104] CA Aix-en-Provence, 2 juin 1993 a retenu l'entente pour une personne ayant remis des cartes bancaires à un contrefacteur pour qu'il procède à leur encodage.

[105] Art. L. 323-7 Code Pénal : « La tentative des délits prévus par les articles 323-1 à 323-4 est punie des même peines. »

[106] Art. L. 323-5 et 6 Code Pénal.

[107] TGI Paris, 5 janvier 1994 à propos du livre de Mark A. Ludwig « *Naissance d'un virus* » qui reproduisait sur support papier les codes sources de quelques programmes malfaisants et les communiquait dans une disquette (www.textfiles.com/magazines/LNOIZ/lnoiz17.txt)

[108] Rappelons que le projet initial visait à réformer le vol, l'abus de confiance et l'escroquerie pour l'ouvrir à une connotation informatique.

d'emprisonnement, le montant des amendes maximales des infractions des articles L. 323-1[109] et suivants du Code Pénal en son article 45, la loi a envisagé la sanction de la « *détention ou la mise à disposition de virus informatique, sans qu'il soit besoin que ledit virus ait été introduit frauduleusement dans un système de traitement automatisé de données* ».

Il résulte du texte même que la nouvelle incrimination vise des actions correspondant à la fourniture, mais aussi à la détention du matériel initialement réprimé. Dès lors, tout logiciel doté d'un accès dissimulé pourrait voir l'utilisateur de l'accès sanctionné sur le fondement de cet article, ce qui ne semble pas être nuisible d'un premier abord, sauf à considérer, d'une part, la portée de cet article au regard des multiples accès à distance à des fins de maintenance et d'administration de nombreux logiciels et, d'autre part, le champ d'application de l'article L.323-1 relatif à l'accès ou au maintien dans un système. Ainsi, chaque utilisateur de logiciel ayant ce type de fonctionnalités[110] serait susceptible de se voir condamné[111]. En effet, il est avéré que de telles fonctionnalités sont spécifiquement réalisées pour permettre un accès à distance dans un système étant donné qu'il s'agit de leur fonction unique et ce, même si la conception de l'accès n'a pas été réalisée dans le but de commettre une infraction. L'interprétation du texte n'est pas aisée car, d'autre part, on peut considérer que par l'expression « *conçue ou spécialement adaptée* », il faut comprendre que, dès la conception de la fonctionnalité, il y avait volonté de réaliser une ou plusieurs des infractions des articles L. 323-1 à L. 323-3 du Code Pénal.

Par ailleurs, Mme Marie Barel fait justement remarquer[112] que le terme de « *détenir* » est purement passif alors que les termes « *importer* », « *offrir* », « *céder* » et « *mettre à disposition* » impliquent une certaine action, voire une création. Elle ajoute, d'autre part, que cette incrimination, visant à sanctionner les comportements préalables à la propagation des programmes viraux, était déjà apparue dans le projet de loi sur la Société de l'Information, mais sans référence aucune à la notion de détention[113]. Il en résulte une appréhension pénale de certains actes préparatoires, non punissables au titre de la tentative, de manière autonome et « *quasi-automatique* » selon les termes même de M Patrick Devedjan, Ministre délégué à l'Industrie mais aussi de l'ensemble du cycle de la pré-vie (conception) et de la vie des programmes viraux.

En outre, l'article vise l'ensemble des dispositifs permettant ou simplement facilitant la commission des infractions en matière de fraude informatique dans la mesure où ils sont « *conçus ou spécialement adaptés pour permettre la commission de l'infraction* ». Il s'agit, pour Mme

---

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

[110] Ces logiciels sont bien plus fréquents que on ne le croit : de simples logiciels de navigation Internet, clients mails disposent de telles fonctions. Alors, que penser des fonctions d'administration via protocole *Telnet* des ordinateurs eux-mêmes ou d'un lien profond vers la partie d'un site Internet réservé à certaines personnes ?

[111] Rappelons que les juges sont peu nombreux à être formé en matière de nouvelles technologies comme nous le montre la solution de l'affaire *Tati/Kitetoa* de la CA de Paris du 30 octobre 2002 rendue au motif de l'accès au site avec un simple navigateur alors que cette fonctionnalité du navigateur, oubliée, n'était documentée que sur des forums dédiés au « *hacking* ».

[112] Marie Barel, *« Nouvel article 323-1 du Code Pénal : le cheval de Troie du législateur », MISC n°14 (2004)*

[113] Article 35 du projet LSI dans sa version du 14 juin 2001.

Barel, de « *l'avènement d'une nouvelle catégorie de biens à double usage* » au même titre que les biens cryptographiques[114]. Pour reprendre notre exemple précédent de l'accès dissimulé, ce dernier est principalement utilisé pour l'administration à distance d'un système, mais il est aussi spécialement utilisé pour accéder sans droits au même système. Un programme viral pouvant mettre en œuvre cet accès (ou une quelconque faille de sécurité) serait, par contre, illégal du fait qu'il a été spécifiquement conçu pour mettre en œuvre cet accès. Par ailleurs, un programme viral installé en connaissance de cause sur sa propre machine pour réaliser certaines tâches serait *de facto* illégal car susceptible, s'il était transmis à un autre système, de l'entraver ou le fausser.

Cela nous apparaît comme relativement inepte car interdisant, sur une simple potentialité d'atteinte, tout un type de programmes ou de fonctionnalités.

En dernier lieu, le texte fait mention de l'expression « *sans motif légitime* », ce qui confie au juge l'entière appréciation de la situation, situation qui sera en pratique, sans aucun doute, confiée aux soins de nombreux experts chargés de définir si le produit informatique utilisé sera, dans notre cas, un code infectieux susceptible de permettre ou de faciliter une infraction ; ce qui, compte tenu de la quasi-assurance de cette qualification, déplacera la solution du litige sur le terrain de l'élément intentionnel dont le législateur fait ici peu de cas. Nous pouvons d'ores et déjà nous poser la question de l'apprentissage de connaissances pouvant permettre ces infractions ; apprentissage effectué dans le but de concevoir ou utiliser les outils permettant d'éviter ces infractions mais qui pourra vraisemblablement être appréhendé par le texte dès lors qu'elles seront formalisées sur un support quelconque.

A titre d'exemple de l'accueil réservé à l'article 45 par le milieu professionnel, M. Eric Filiol, chef du laboratoire de virologie et de cryptologie de l'Ecole Supérieure d'Application et des Transmissions, dans un récent article [115] se demande si les activités des laboratoires en matière de virologie informatique pourraient encore continuer, étant donné que la notion de « *motif légitime* » sera appréciée au cas par cas, laissant les experts prendre la décision finale et mettant en péril, aussi bien l'enseignement de la matière, que la recherche antivirale. Il ajoute que la publication des failles des logiciels sera soumise à la même disposition, ce qui risquerait de provoquer la censure des chercheurs en ce domaine, les utilisateurs finals en faisant, en dernier lieu, les frais.
[…]

On ajoutera que M. René Trégouët, rapporteur du projet de loi, lors des débats en seconde lecture devant le Sénat, rappelait que cet article n'avait « *ni pour vocation, ni pour effet, de permettre la sanction pénale d'internautes non avertis, qui détiendraient malgré eux un virus informatique ou qui utiliseraient à des fins illicites des logiciels d'accès à des ordinateurs ou serveurs distants* ». Mais, si le droit français, en l'article L. 121-3 du Code Pénal, précise qu'un délit suppose

[114] Pour plus d'informations, consulter : http://www.wassenaar.org. Succinctement, en France, les biens cryptographiques étaient considérés comme des matériels de guerre de deuxième catégorie jusqu'à la loi LRT du 29 décembre 1990, puis, après comme des biens à double usages : utiles pour la sécurisation des réseaux mais objets de délits passé une certaine complexité, en l'occurrence 128 bits (pour la cryptographie à clés secrètes uniquement).
[115] Jean-Marc Manach, ZDNET France, Jeudi 10 juin 2004 « *Quand un officier supérieur de l'armée tire à boulet rouge sur la LCEN* ».

effectivement une intention de le commettre, il semble, à la lecture du texte, qu'il faille, pour comprendre ceci, se référer plus à l'esprit de la loi qu'à sa lettre même ; ce qui ne peut être que source de conflits futurs sur ce terrain.

4. La loi « Informatique et libertés » du 6 janvier 1978

A titre accessoire, afin de terminer notre panorama des textes susceptibles d'appréhender les phénomènes malicieux en droit français, il nous faut citer la loi « Informatique et libertés » du 6 janvier 1978, modifiée par celle du 6 août 2004[116].

En effet, la loi soumet ceux qui procèdent à des traitements, automatisés ou non, de données à caractère personnel, à certaines obligations de déclaration ou d'autorisation préalable, sous peine de sanctions pénales. Bien que l'hypothèse soit marginale, il semble qu'un mécanisme viral qui collecte de telles données pour les faire inscrire dans un fichier soit susceptible d'être appréhendé par ce texte, les dispositions de l'article 4[117] ne pouvant s'appliquer en l'espèce.

Il est entendu que, par données personnelles, on comprend « *toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres* », c'est-à-dire les données attachées à la personne même mais aussi celles attachées au matériel qu'elle utilise. A ce titre, la Commission Nationale de l'Informatique et des Libertés considère, en se basant sur la directive du 24 octobre 1995 et sur la loi de 1978 qui encadrent la collecte de telles informations, que l'adresse IP (pour « *Internet Protocol* »), à savoir le numéro d'identification d'un système sur le réseau Internet via le protocole TCP/IP, est une donnée personnelle. Dès lors, un mécanisme viral qui collecterait ou scannerait et utiliserait ces adresses IP afin d'y installer, par exemple, un serveur proxy destiné à lui permettre une propagation plus rapide ou à favoriser l'envoi de courriers électroniques non sollicités pourrait être appréhendé par les articles 6 et suivants de la loi « Informatique et libertés ». Par ailleurs, on peut penser que les adresses MAC (*Medium Access Control*) des périphériques réseaux se verront appliquer la même solution.

5. Aperçu international du droit appliqué aux mécanismes infectieux

La criminalité informatique n'est plus et n'a sûrement jamais été cantonnée à un seul pays. Il s'agit d'un risque, à défaut, d'une menace internationale, comme le démontre le souci de l'ONU de le rappeler lors des dixième et onzième Congrès des Nations Unies pour la Prévention du Crime et le Traitement des Délinquants. Les rapports issus de ces Congrès citent les virus au titre de la cybercriminalité montante et du piratage/sabotage informatique et enjoignent les Etats à se doter de législations aptes à punir ce phénomène (a). Cependant, ces derniers ont rencontré l'obstacle du caractère transnational de ces infractions. Quelques pistes internationales ont donc été avancées dans le sens de la résolution de ce problème (b).

---

[116] Pour le texte intégral : http://www.legifrance.gouv.fr/texteconsolide/PPEAU.htm

[117] Article 4 : *« Les dispositions de la présente loi ne sont pas applicables aux copies temporaires qui sont faites dans le cadre des activités techniques de transmission et de fourniture d'accès à un réseau numérique, en vue du stockage automatique, intermédiaire et transitoire des données et à seule fin de permettre à d'autres destinataires du service le meilleur accès possible aux informations transmises*. »

a. Quelques exemples nationaux

Ainsi, les Etats Unis disposent, au niveau fédéral du « *Conterfeit access device and computer fraud abuse act* » de 1984, du « *Computer Fraud and Abuse Act* » de 1986[118], ainsi que le « *National Information Infrastructure Protection Act* » du 27 août 1996[119].

La loi y sanctionne le fait de transmettre, par un support physique ou un réseau, de manière intentionnelle, un programme, une information, un code ou une commande susceptible de provoquer des dommages à un ordinateur[120]. Il en résulte l'appréhension pénale de la diffusion des mécanismes viraux au même titre que le nouvel article L.323-3-1 du Code Pénal en France. Par ailleurs les législations des Etats de la Fédération ont pris des mesures complémentaires, l'état de New-York instaurant, par exemple, le 6 juin 1993, le crime de « *violence informatique* »[121] visant à prendre en compte l'importance financière des dommages indirects subis par la victime du fait de l'utilisation d'un outil informatique.

Le Canada, suite à l'affaire *McLaughlin* relative à une fraude au service de télécommunication de l'Université d'Alberta[122] qui démontra certaines lacunes de leur code criminel en matière d'utilisation non autorisée d'un ordinateur, suit cet exemple. Ainsi, les articles 342.1 et 430(1.1) du Code Criminel créent, le 4 décembre 1985, deux nouvelles infractions : l'utilisation non autorisée d'un ordinateur et le méfait de données informatiques. De la même manière qu'en France, le législateur a préféré s'attacher à la notion de données plutôt qu'à celle d'information, évitant ainsi la question de son appropriation.

Ainsi, y est passible d'un emprisonnement de dix ans, l'obtention frauduleuse directe ou indirecte des services d'un ordinateur, l'interception d'une fonction d'un ordinateur[123] ou l'utilisation d'un ordinateur aux fins de commettre cette obtention ou cette interception. Comme pour la France, il s'agit d'un délit formel couvrant de nombreuses possibilités d'action sur un système informatique et permettant la répression de toute utilisation non autorisée accomplie frauduleusement[124].

Parallèlement, en raison du caractère dangereux de ces mécanismes, certains états ont opéré des distinctions inédites. Ainsi, l'Etat de Singapour a amendé en 1999 son « *Computer Misuse Act* » et différencié les systèmes « sensibles » des autres systèmes. Ainsi, les peines encourues en cas d'intrusion, de quelque nature qu'elle soit, dans des systèmes « protégés », tels que ceux de la

[118] Voir : http://bar.austlii.edu.au/au/other/crime/123.html pour le texte original.
[119] Voir : http://www.usdoj.gov/criminal/cybercrime/s982.htm, pour le texte original.
[120] Section 1030 : Fraud and related activity in connection with computer.
[121] William B. Bierce, « *Le crime de violence technologique à New-York* », Expertises 1998.
[122] R. c. McLaughlin, 1980, 2 R.C.S.331, Comm Herbert et Pilon, Ottawa, SRBP, Ministère des Approvisionnements et Services Canada, 1992, pp. 11-13.
[123] Sur ce point, la législation canadienne est plus complète de celle de la France puisqu'elle permet d'appréhender de manière pénale l'interception d'ondes électromagnétiques telle que les systèmes issus des dispositifs « *Tempest* » (ou *phreaking* de Van Eck).
[124] Trudel, Pierre, France Abran et al., « *Droit du Cyberespace* », Montréal, éd.Thémis, 1997.

fonction publique, des banques et autres institutions liées à la sécurité internationale, ont été augmentées[125].

b. La Convention Européenne sur la Cybercriminalité

La Convention Européenne sur la Cybercriminalité a pour objet de compléter les traités et accords multilatéraux ou bilatéraux de coopération en matière pénale existant entre les Etats. Ainsi, la Convention Européenne d'Extradition du 13 décembre 1957, la Convention Européenne d'Entraide Judiciaire en matière pénale du 20 avril 1959, son protocole additionnel du 17 mars 1978, furent particulièrement visés lors de la rédaction de la convention. Nous noterons que, parallèlement, la Commission Européenne a adopté le 22 avril 2002 une " proposition de décision cadre " sur la lutte contre la cybercriminalité.

Entrée en vigueur le 1er juillet 2004, la Convention du Conseil de l'Europe sur la cybercriminalité est présentée comme le « *premier traité international sur les crimes commis via l'Internet et les autres réseaux informatiques* »[126] et vise à mettre en place une politique pénale commune en matière de cybercriminalité, notamment dans le domaine de la fraude informatique. Ainsi, elle s'efforce de faciliter la conduite d'enquêtes pénales dans le monde virtuel.

Plus précisément, les articles 16 et 17 imposent aux Etats "*la conservation rapide des données stockées*" et les obligent à adopter les mesures visant à pouvoir enjoindre à une personne ou à une entreprise la conservation de certaines données informatiques stockées ou des données de connexion qui pourraient être relatives à une infraction pénale. Ces mesures devaient permettre la préservation de certaines données spécifiées en leur état originel, qu'il s'agisse de données de trafic ou de données de contenu, afin d'empêcher toute perte d'information, mais aussi la traçabilité des ces informations sur les réseaux informatiques. Par ailleurs, cette mesure, d'une durée maximale de 90 jours renouvelable, pouvait être gardée confidentielle afin de protéger l'issue des investigations.

En outre, l'article 18 prévoit *"des injonctions de produire des données"* afin de favoriser la communication aux autorités compétentes de tout type de données stockées dans un système d'information.

Au surplus, le titre 4 de la Convention prévoyait des dispositions visant à faciliter les perquisitions et saisies de données informatiques stockées dans un système informatique[127].

Ainsi, les autorités perquisitionnantes qui pensent que les données recherchées sont stockées dans un autre système informatique, pourront être en mesure, si ces données sont légalement accessibles à partir du système initial, d'étendre la perquisition à cet autre système. Par ailleurs,

---

[125] Voir : http://www.un.org/french/events/10thcongress/2088hf.htm
[126] Communiqué officiel du Conseil de l'Europe (http://www.k-otik.com/news/03.18.eucybercrim.php).
[127] Le rapport explicatif précise que : « *Etant donné qu'en application de l'article 1, l'expression "système informatique" désigne "tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés", le paragraphe 1 concerne la perquisition d'un système informatique et de ses composants apparentés pouvant être considérés comme constituant ensemble un système informatique distinct* ».

les personnes ayant une connaissance du fonctionnement du système d'information objet des mesures de perquisition et de saisie pourront être forcées à une coopération avec les enquêteurs.

Il en résulte qu'au regard, tant de notre législation nationale que des diverses initiatives au niveau européen et mondial, les programmes offensifs sont appréciés d'une manière globale et unanimement pénalisés, sur divers fondements.

Ainsi, la législation française sanctionne les virus pour la forme et non pour les effets, ce qui condamne *a priori* les infections bénéfiques. En effet, la simple apparition d'une image sur un écran peut faire entrer le programme viral qui la met en œuvre dans le champ des infractions pénales spécifiques des articles L. 323-2-1 et suivants du Code Pénal. Pourtant, la même image, mise en œuvre par le système d'exploitation ou par un logiciel d'application, dont l'apparition n'était pas plus consentie par le maître du système que dans le cas précédent, ne pourra se faire appréhender par ces même textes. Afin de résoudre cette iniquité, nous allons dorénavant analyser plus précisément les diverses implications d'un mécanisme viral «bénéfique » ou « positif ». Les conséquences d'un tel virus sont en effet, parfois, extrêmement lourdes[128].

[128] Ainsi, le décret n°2002-692 du 30 avril 2002 prévoit que « *Tout document électronique envoyé par un candidat dans lequel un virus informatique est détecté par l'acheteur public peut faire l'objet par ce dernier d'un archivage de sécurité sans lecture dudit document. Ce document est dès lors réputé n'avoir jamais été reçu et le candidat en est informé* ». Dès lors que l'offre est accompagnée d'un virus, elle devient nulle.

Deuxième partie - Des infections juridiques aux virus bénéfiques

Par définition, un virus n'a rien de particulièrement néfaste[129]. En 1986, Fred Cohen affirmait déjà que les virus « utiles » ou « bénéfiques » était une possibilité réelle[130]. Toutefois, l'idée d'implémenter un programme de type viral sur un système soulève de nombreuses difficultés. Afin de les résoudre, nous allons tout d'abord envisager la qualification et le régime juridique de ces virus « bénéfiques » (A) puis développer les solutions qui pourraient contribuer à leur créer une « vie » juridique autonome du droit pénal (B). En effet, il nous apparaît que résoudre le problème des virus (nuisibles et « bénéfiques ») ne peut se faire qu'en prenant en considération, à la fois et une fois encore, la dimension juridique et technique du problème.

Section A - Le virus informatique bénéfique : une transposition de l'existant biologique

Afin d'étudier plus précisément les « infections informatiques bénéfiques », il est nécessaire de définir exactement ce dont il s'agit (2), puis d'expliquer ce que nous appellerons la notion de « positivité virale » (3), avant de définir les caractéristiques essentielles de ces infections informatiques bénéfiques (4). Cependant, en matière de virologie informatique, les termes font souvent référence à la virologie traditionnelle, c'est-à-dire à l'étude des virus biologiques. En premier lieu, nous nous attarderons donc sur la comparaison des virus informatiques avec ces derniers afin d'obtenir une définition satisfaisante (1).

1. L'analogie virus biologique / virus informatique

Cette comparaison désormais classique apparaît nécessaire[131]. En effet, la quasi-totalité du vocabulaire utilisé en matière de virologie informatique provient du domaine biologique. Toutefois, il s'agira d'identifier aussi bien les différences que les ressemblances entre ces deux mécanismes parasites, sur le plan interne (a) ou externe (b), afin de savoir si cette comparaison s'impose d'elle-même ou si, au contraire, il faut s'en détacher pour appréhender de manière adéquate ce qui pourrait être exactement une infection informatique bénéfique (2).

a. Les éléments internes de la comparaison

A ce titre, une présentation sous forme de tableaux nous semble être plus que naturelle, car elle permet une appréhension plus synthétique et plus explicite de la comparaison[132]. Nous comprenons par éléments internes ceux qui sont inhérents aux virus mais aussi leur

---

[129] Toutefois, nombreux sont ceux qui considèrent que la consommation des ressources du système inhérente à tout mécanisme viral constitue déjà une nuisance. Nous reviendrons sur la question.

[130] Il avait d'ailleurs offert une prime de 1000$ à quiconque développerait un tel virus mais, en dépit de quelques essais, il n'y a jamais eu de suite.

[131] Afin d'effectuer cette comparaison, nous nous fonderons principalement sur les travaux de John Stewart, professeur en sciences cognitives, consultables en partie sur : http://www.vieartificielle.com et ceux de Rod Daniels, directeur d'un laboratoire de recherche en virologie au *National Institue for Medical Research* (GB) et Jack Clark, consultant en technologie antivirale chez *Network Associates* (travaux intitulés « *Virtual Technology : The first Examination of the parallels between cyberviruses and human viruses* »).

[132] Les ressemblances seront légèrement grisées tandis que les différences resteront sur fond blanc.

comportement (et par la même, *de facto*, le comportement de leur concepteur en ce qui concerne les virus informatiques).

Virus Informatique	Virus Biologique
Il s'agit d'un programme composé d'une série d'instructions (octets) et d'un sous-programme de reproduction.	Il s'agit d'un micro-organisme doté de son propre patrimoine génétique composé de nucléotides (brin d'ADN ou d'ARN suivant le type de virus).
- Les programmes infectés génèrent de nouveaux programmes viraux.	- Une cellule contaminée produit des virions, progéniture du virus initial[133].
- Ils nécessitent une exécution pour leur dissémination.	Ils se multiplient uniquement dans des cellules vivantes.
- ne peut agir que sur certains formats spécifiques. En leur absence, il demeure inactif.	- est spécifique d'une famille de cellules (ex: le virus HIV s'attaque aux cellules du système immunitaire, les lymphocytes).
- ne peut se reproduire que par duplication de son code viral.	- se reproduit également par réplication de son code génétique au sein d'autres cellules.
- se multiplie uniquement via un programme ou un fichier infecté, sa propagation est directement liée au vecteur qu'il infecte le principe du ver diffère en ce point).	- ne peuvent exister isolés ; nécessitent une cellule hôte dont elle pourra utiliser la structure pour se répliquer.
- modifie les actions que peut réaliser un programme.	- modifie de l'information génétique de la cellule contaminée.
- peut se déclencher immédiatement ou après un temps de latence.	
- énergie électrique fournie par le système.	- énergie bioélectrique puisée au sein de la cellule contaminée.
- La dissémination s'effectue de manière optimale par courrier électronique[134].	- Le mécanisme de propagation le plus efficace est un vecteur aérien.
- peut se transformer, devenant ainsi difficile à détecter et peut disparaître du programme hôte après s'être multiplié.	- peut se transformer afin de ne pas être détecté par les défenses immunitaires de l'organisme infecté et peut aussi disparaître de la cellule hôte après s'être multiplié.
- Routine de lutte contre la surinfection : un programme qui aura déjà été en contact avec un virus ne pourra pas être contaminé une seconde fois par ce même virus	Il en sera de même pour le virus biologique, puisque son contact avec un organisme déclenche une réaction de séropositivité.
- les virus informatiques ne sont pas réellement capables d'évolution. Il est toutefois possible simuler cette évolution via le développement un sous-programme d'apprentissage inclus dans le virus initial.	- Capacité à évoluer, à s'adapter à leur environnement, à se mettre « en sommeil ».
D'une manière générale, tous domaines confondus, les virus les plus dangereux sont les plus petits en terme de taille[135].	

[133] Dans ce cas de réplication, les virus peuvent produire des dégâts irréparables, programme inutilisable et cellule hôte phagocytée (cellule dont le code génétique a été altéré de manière irrémédiable).

[134] Pour certains, il s'agit de mécanismes équivalents dans deux mondes différents : matériel et logique. Pour nous, il existe une différence entre les deux : l'air correspond à un élément passif vital de la vie biologique, qui serait plus à rapprocher en ce cas des flux de données (plus ou moins maîtrisés) des protocoles de communication constituant l'Internet que du courrier électronique.

Un virus informatique peut être « pathogène » dans un système d'exploitation donné mais bénin dans un autre.	Dans de nombreux environnements, le virus biologique peut être pathogène, mais dans d'autres demeurer inoffensif.
Un nombre important de virus biologiques et logiques proviennent de l'Asie et font route vers l'ouest (pour les premiers, notamment à cause de la densité humaine de quelques régions, pour les seconds, probablement à cause de la hausse rapide du niveau technologique et de la relative jeunesse des populations habitants ces régions).	
De manière subséquente à leur nature parasitaire, les cibles privilégiées des virus sont les systèmes logiques ou immunitaires les plus faibles et les moins protégés.	
- Pas d'émergence[136].	- Emergence, c'est à dire qu'une vie organique aura une réaction que nous ne sommes pas capables de prévoir à 100%, même pour des êtres unicellulaires.
- La propagation et les dégâts occasionnés par les deux types de virus sont similaires. De plus, on note une ressemblance dans leur mode d'action. De même les méthodes de prévention, détection, vaccination et destruction des deux types de virus sont souvent comparables.	

On ajoutera que sur de nombreuses notions, le domaine informatique a son pendant biologique : virus luttant spécifiquement contre un antivirus/virus de code source et rétrovirus ; virus binaires et interactions virales, polymorphisme et mutation, virus latents et porteur sain[137], antivirus génériques et antigènes.

Toutefois, en matière de biologie, on observera qu'il n'existe pas d'utilisation de virus comme vecteur de vaccination alors qu'en matière informatique, la base de signature d'un logiciel antivirus remplit ce rôle (cf. II/B/1/b pour comprendre les mécanismes des logiciels antivirus).

On remarquera, en conséquence, les nombreuses similitudes entre les virus biologiques et logiques ; similitudes qui ne vont toutefois pas jusqu'à la totale fusion des caractéristiques essentielles de ces deux types de mécanismes, mais qui laissent à penser que les virus pourraient être les bactéries des « *backbones* » informatiques, leurs premiers parasites logiques.

b. Les éléments externes de la comparaison

Virus Informatique	Virus Biologique
Virus biologiques et virus informatiques sont classés en fonction de leur pathogénéité.	
La menace logique est prise en charge par des organismes privés : les éditeurs d'antivirus.	Ce sont des organismes nationaux ou internationaux, généralement publics ou dotés de fonds publics qui ont compétence pour analyser ces virus.

[135] Pour M. Paget, plus un virus informatique est important en terme de taille, moins il se propage car, même s'il est techniquement plus complexe, il est plus facilement décelable. C'est pourquoi la majorité des virus véritablement dangereux font entre 300 octets et 30 kilo-octets environ.

[136] Dans le cas d'un virus polymorphe, certains considèrent qu'ils font preuve un comportement émergeant caractérisé par leur capacité à réécrire tout ou partie de leur code et donc en « écrivant » un code autre que celui du concepteur. Toutefois, nous considérons que les fonctionnalités/réactions n'étant pas altérées il n'y a pas d'émergence véritable.

[137] E. Filiol, op. cit. *supra*, p 78.

Les deux menaces sont traitées de manière mondiale avec une coopération certaine entre les différents organismes.	
La prévention (installation de logiciels ou matériels de sécurité)apparaît comme le meilleur remède.	L'hygiène et la vaccination (quand cela est possible) sont les meilleurs moyens pour éviter l'infection par un virus.

La comparaison est ici moins pertinente que celle concernant les éléments internes à ces mécanismes. En effet, sur le plan externe, il existe une certaine automaticité de la comparaison, les structures humaines des technologies de l'information s'étant calées sur les structures déjà existantes en matière biologique afin d'optimiser leur manière de réagir et de partir sur un fondement déjà connu.

Bien que l'on puisse penser que les virus sont le pendant logique d'un début de vie artificielle[138], une sorte d'organisme monocellulaire informatique, la question pose d'importants problèmes, tant scientifique, qu'éthique ou philosophique, dont nous ne pouvons malheureusement qu'en donner un bref aperçu (Annexe 2). Nous pouvons toutefois ajouter sans coup férir que les premiers virus furent les objets d'études réalisées dans le cadre de l'intelligence artificielle.

Il résulte de cette comparaison que nous pouvons considérer qu'un virus biologique bénin, voire non-pathogène, serait l'équivalent d'une « infection informatique bénéfique ». Bien que les termes de « non-pathogène » et de « bénéfique » ne soit pas exactement similaire, c'est ce qui semble avoir le sens le plus proche, au vu de la démonstration que nous voulons mener. Partant de ceci, il nous est maintenant moins délicat de définir une telle « infection informatique bénéfique ».

2. Définition des « infections informatiques bénéfiques »

Afin de définir précisément ce dont il s'agit, il faut, nous semble-t-il, prendre un parti pris dans la question vue précédemment, à savoir le statut de « vie artificielle » du virus informatique. Disposant de la capacité de se reproduire, nous les analyserons ainsi comme une sorte de prémices d'une vie artificielle, entité non encore douée d'une vie autonome car trop simple mais dont les potentialités en font une sorte d'outil génétique informatique pouvant aboutir à la naissance de l'étincelle de chaos nécessaire à la vie.

Tout en gardant à l'esprit le fait d'avoir une définition générale qui ne connote aucunement un quelconque effet néfaste, utilisable en matière de sécurité informatique, nous nous fonderons sur les travaux de M. Eric Filiol, Adleman et Cohen pour la rédiger. Ainsi, une infection informatique bénéfique pourrait être définie comme suit :

« *Un programme auto-reproducteur non neutre et, à défaut, évolutif s'installant au sein d'un système d'information, librement consenti ou non, et qui, dans un environnement donné et défini, est capable de modifier d'autres programmes de manière à ne provoquer sur ledit système aucun comportement susceptible de porter atteinte à son intégrité et/ou sa disponibilité* ».

[138] Voir sur ce point, l'ouvrage de Mark A. Ludwig , « *Mutation d'un virus »,* éd. Adisson Wesley, 1994 [Voir 12].

Dès lors, quelques remarques s'imposent. Ainsi, nous avons choisi dans cette définition d'éluder les programmes simples (cf. I/A/2/a), car Léonard Adleman ne les considérait pas comme de véritables infections. En effet, on ne peut pas considérer qu'une bombe logique, par exemple, soit considérée comme une application de l'ensemble des programmes sains vers l'ensemble des programmes infectés comme un virus peut l'être[139]. Pour désigner l'ensemble des programmes simples et auto-reproducteurs, on préfèrera le terme de « parasite informatique ».

Par ailleurs, « non neutre » signifie que le programme a une réelle action sur le système, qu'il n'a pas pour seule fonction de se reproduire et de rester indéfiniment en un état de torpeur logique et donc, comme nous le verrons postérieurement, que, dans une certaine mesure, il est doté d'une charge finale « positive »[140]. En cela il est différent du seul terme « non pathogène ». De même, le terme d'«évolutif » fait référence aux thèses darwiniennes de l'évolution et laisse à penser qu'il existe une certaine complexité des programmes mais aussi qu'ils sont capables de survivre en milieu hostile (face aux mécanismes des antivirus par exemple), soit par une méthode de furtivité, soit par une accréditation d'accès aux ressources du système par le système d'exploitation. En outre, l'expression « librement consenti ou non » ajoute l'idée que le programme peut être lui-même voulu par l'utilisateur du système ou qu'il peut ne pas avoir conscience de sa présence, de la même manière que l'ensemble des sous-programmes du système d'exploitation ou des logiciels d'applications par ailleurs.

En dehors de l'expression « *susceptible de porter atteinte à son intégrité et/ou sa disponibilité* », les termes sont compréhensibles et ne dénotent aucune signification particulière. Cette dernière expression fait donc état d'une absence de nuisance au système lors du fonctionnement du programme, mais aussi de l'absence de la simple potentialité de cette nuisance lorsque le programme est juste présent et inactif sur le système. Restera alors à définir, au cas par cas, ce que l'on considèrera comme une nuisance ou ce que l'on considérera comme une gêne, soit non imputable au programme, soit négligeable par rapport aux ressources du système hôte ; ce qui pourrait être appréciable, notamment, en fonction de la nature et de l'ampleur du consentement éclairé de l'utilisateur.

Il apparaît donc qu'un « virus positif » n'est pas simplement un programme intrusif utilisé à des fins bénéfiques plutôt qu'à des fins de destruction mais véritablement un entité disposant de l'autonomie nécessaire à sa reproduction et sa survie dans un environnement préalablement défini par son concepteur et dont les effets sur celui-ci ne sont pas néfastes, que cela soit de manière volontaire ou non.

Cet effet « non-néfaste » ou « positif » est toutefois à préciser.

3. La notion de « positivité virale »

S'agissant de cette notion de « positivité virale », il convient préalablement d'expliciter ses fondements (a) avant d'appréhender la notion d'effet « positif » (b).

---

[139] Léonard Adleman, op. cit. *supra* note n° 12.
[140] Voir la distinction code auto-reproducteur/charge finale (cf. II/A/3/a).

a. Genèse de la notion

La notion de « positivité virale », fait pour un mécanisme auto-reproducteur d'avoir un effet « bénéfique », apparaît comme étroitement liée à la dissociation du code auto-reproducteur et de la charge finale.

- La dissociation code auto-reproducteur/charge finale

Au sein d'un organisme viral informatique, composé d'une série d'instructions primaires, nous pouvons en effet séparer de manière artificielle les routines et portions de code associées au mécanisme de reproduction qui, comme nous l'avons vu est de l'essence même du virus, de celles qui peuvent être associées à la charge finale (« *payload* ») c'est-à-dire des routines offensives, couplées ou non à un mécanisme de déclenchement différé, la part du code viral qui produit les effets du virus. Cette charge finale trouve généralement et actuellement sa matérialisation dans une application de type bombe logique à vocation nuisible. Cependant, dès lors que l'on intègre à cette charge finale une dimension « positive » avec, par exemple, une application « utile », nous pourrions entrer dans le champ de la notion de positivité virale.

Toutefois, il convient de préciser que si, en théorie, le code auto-reproducteur est neutre, éthiquement parlant, certains phénomènes viraux constituent en eux même un programme de type charge finale. C'est notamment le cas des vers *CodeRed* et *Saphirre* qui, afin de procéder à leur reproduction, scannent les ports des systèmes distants afin de voir où ils pourraient se copier. Ce faisant, ils encombrent les réseaux de requêtes inutiles et utilisent de manière non négligeable les ressources du système hôte et des systèmes distants. Ces vers ont, *de facto*, un effet nuisible, sans qu'il soit besoin d'y inclure une charge finale autre. Le mécanisme infectieux constitue en lui-même la charge finale.

Pour reprendre notre définition des infections informatiques bénéfiques, en l'espèce, il y aurait atteinte à la disponibilité d'un système[141], dans la mesure où les ressources de ce système sont utilisées de manière importante. De tels vers ne sauraient donc entrer dans le champ de cette définition, et ce, même en l'absence de toute charge finale autonome et nuisible.

- Les applications susceptibles d'utiliser un mécanisme viral

Au titre de la nomenclature des diverses infections informatiques, quelques exemples d'applications où un mécanisme viral pourrait être introduit ont déjà été donnés (cf. I/A/2). Il nous revient dès à présent de les développer, étant précisé que les infections informatiques dites « simples » ne seront abordées ici qu'à titre accessoire.

Même si aucune application commerciale n'a encore été trouvée à ces mécanismes autoreproducteurs, nous pouvons néanmoins en donner quelques exemples pratiques. Ainsi, nous pouvons citer le ver *Nachi* qui, en août 2003, était destiné à réparer les ordinateurs infectés par le ver *Blaster* en téléchargeant les derniers correctifs de la société *Microsoft* et qui, en février 2004,

[141] Nous noterons qu'en ce cas, le système indisponible n'est pas nécessairement le système hôte mais peut être un serveur distant chargé de répondre aux multiples requêtes du vers.

revenait pour le ver *Mydoom*[142] dans une seconde version mais aussi le virus compacteur *Crunsher* apparu en 1993. D'une manière générale, nous pouvons distinguer les applications qui améliorent un procédé ou un savoir-faire déjà existant des applications nouvelles.

Ainsi, les premières peuvent s'analyser en le franchissement d'une étape supplémentaire dans l'automatisation d'un procédé informatique[143], un ajout d'un mécanisme de dissémination ou de diffusion à un processus déjà existant quel qu'il soit. Nous pourrions donc utiliser semble-t-il un tel mécanisme pour l'ensemble des tâches d'administration de réseau afin de procéder de manière automatique à la mise à jour des logiciels applicatifs ou d'exploitation, au téléchargement et à l'installation des correctifs[144], surveillance des systèmes, protection des données, mais aussi en matière de publicité[145], de récupération licite de données ou de recherche d'informations ainsi que tout processus nécessitant une intervention humaine minimale, par exemple pour des questions de secret ou de fiabilité. Nous noterons que dans de nombreux cas, leur mise en œuvre reste délicate mais pas impossible (cf. II/B/4).

Par ailleurs, de nombreuses applications seraient susceptibles d'être mises en œuvre par un tel mécanisme, dans une certaine mesure, intrusif. Ainsi, en matière de lutte contre la criminalité, on peut largement imaginer le principe d'un virus chargé de récupérer des données sur l'ordinateur distant d'un prévenu dans le cadre d'une télé-perquisition, d'automatiser la recherche pertinente d'une personne[146] en fonction de certains éléments. Par ailleurs, en d'autres matières, on peut aisément penser à d'autres applications de ces codes viraux : marquage numérique de données[147], partage de ressources, utilisation étatique à des fins de défense ou militaire[148] …

Les possibilités sont aussi nombreuses[149] que les abus qui pourraient en résulter et qui forment aujourd'hui l'essentiel de la matière. C'est ainsi qu'il convient de définir véritablement la notion de bénéfice en matière virale et préciser quelques pistes permettant l'existence d'un virus « bénéfique ».

b. Appréciation de la vie juridique des virus bénéfiques

---

[142] Nous ajouterons que, exploitant lui même une vulnérabilité du système d'exploitation et malgré une intention initiale louable, il avait provoqué d'importants problèmes au sein des entreprises. Dans sa première version, il s'agissait tout de même le troisième ver le plus diffusé en 2003.

[143] Pour rappel, la légende veut que le mot « *informatique* » soit la contraction de « *information automatique* » ce qui connote largement une idée d'automatisation quant aux traitements de données.

[144] En effet, la mauvaise gestion des correctifs de sécurité permet au nombreux virus exploitant une faille déjà connue et souvent documentée de proliférer.

[145] On peut imaginer le cas d'un vers faisant apparaître de manière autonome une bannière de publicité qui se désactive à la fin de la campagne publicitaire, étant entendu qu'en ce cas, le « bénéfice » d'un tel virus reste ténu.

[146] Ce pourrait être le cas d'un ver qui en fonction des données de la personne va « réagir » et ne chercher, non pas, dans l'ensemble des bases mais seulement sur certaines, connues ou inconnues au moment de la conception du ver, et dont il s'assurerait de la mise à jour de manière automatique.

[147] Par exemple en marquant tout donnée dont la signature (obtenue par exemple par une fonction de hachage MD5) correspond à la donnée initiale, et ce même après diffusion des données sur le réseau.

[148] Nous pouvons citer le ver Magic Lantern, révélé par le FBI le 6 novembre 2001, qui installait un cheval de Troie de type « *keylogger* » afin d'obtenir plus facilement des mots de passe et des clés de chiffrement dans le cadre du contre-espionnage et de la lutte contre le terrorisme.

[149] Parallèlement, les possibilités d'action de ces virus sont peu nombreuses : au moment de la mise sous tension de l'ordinateur, de son accès au réseau, d'un flux entrant ou sortant de données (E. Filiol, op. cit. *préc.*).

Au vu des éléments de réponses déjà apportés, la notion de virus ou de programme auto-reproducteur est maintenant connue. Il reste cependant un point en suspens. En effet, dire que le virus doit être bénéfique pour être accepté socialement ne suffit pas. Il est nécessaire de définir cette notion de bénéfice appliqué aux mécanismes viraux, cette notion étant subjective et étant appliquée par nature à une personne ou une chose qui va tirer parti de ce bénéfice.

En effet, il n'existe pas réellement « d'effet positif » en tant que tel s'agissant des virus, ces derniers, comme tout autre programme, ne nous semblant pas de nature à présenter un bénéfice pour l'ensemble des intérêts particuliers. En tout état de cause, il existerait cependant un effet positif en relation avec la notion d'intérêt général. Il s'agira notamment du cas où un virus est utilisé en matière de téléperquisition. Nous pouvons supposer que le propriétaire du matériel logique, objet de la téléperquisition, ne tire aucun bénéfice du virus, mais que, dans ce cas, l'intérêt général, via la mise en œuvre d'un des prérogatives régaliennes de l'Etat, prédomine. Il semble donc que l'on doive déjà faire une nuance quand à la notion de « positivité virale ».

Par ailleurs, à l'inverse, nous ne pouvons pas considérer comme « bénéfique » un programme viral qui ne servirait les intérêts particuliers que d'une seule entité. En ce cas, tout virus pourrait être considéré comme tel car, servant au moins, on peut le supposer, les intérêts de leur(s) concepteur(s), qu'il s'agisse d'un intérêt pécuniaire ou simplement d'un intérêt en terme de reconnaissance sociale. Entre ces deux extrêmes, il nous apparaît que pour obtenir une solution satisfaisante, il nous faille opérer une distinction suivant le degré et la nature de l'intégration du virus dans le système. Ainsi, nous pouvons distinguer les programmes spécifiquement désirés par le maître du système, de ceux inclus dans un logiciel et, finalement, de ceux non désirés. Cette distinction est, remarquons-le, en étroite liaison avec celle du consentement[150] de l'utilisateur du système.

Ainsi, pour un programme viral spécifique ou un programme dont la fonctionnalité principale est issue d'un mécanisme viral, manifestement désiré par l'utilisateur, la notion de bénéfice serait amoindrie. En effet, au même titre que tout autre programme, le virus a été accepté dans son mode de fonctionnement et ses finalités. Dès lors, l'utilisateur qui estime le virus non bénéfique ne pourrait se retourner contre son concepteur que dans la mesure de la responsabilité contractuelle inhérente à la licence d'utilisation de ce programme ou dans le cadre de la responsabilité délictuelle de droit commun. Dans un tel cas, de la même manière qu'il n'existe pas de régime particulier applicable aux différentes techniques de programmation, il n'y a pas lieu de distinguer un programme auto-reproducteur d'un programme « simple »[151].

S'agissant d'un programme viral inclus dans un logiciel plus complexe, la part du consentement nécessaire à la mise ne œuvre légitime du sous-programme viral nous semble déjà plus importante. En effet, la fonctionnalité du logiciel issue du mécanisme viral est ici accessoire au logiciel. Dès lors il convient de différencier la nature de cette fonctionnalité suivant qu'elle

[150] Nous entendons le terme de consentement comme un consentement spécifique au fonctionnement d'un mécanisme viral en tant que tel.
[151] Nous nous référons expressément sur ce point au principe général de neutralité technique de la loi pour fonder notre démonstration.

s'insère dans celles plus générales du logiciel ou qu'elle en diffère très sensiblement. Dans le premier cas, il n'y a pour nous, comme précédemment, pas lieu de distinguer un mécanisme viral d'un mécanisme ordinaire. En effet, dire que l'on peut refuser un tel mécanisme reviendrait à dire que l'on peut dissocier, au sein même du logiciel, ses différentes composantes. Or, le logiciel fait l'objet d'une licence générale d'utilisation matérialisant le consentement de l'utilisateur. L'argument selon lequel le mécanisme viral était occulté au consentement initial de l'utilisateur est sans fondement, car cela reviendrait ici aussi à considérer une simple technologie comme néfaste, les composantes d'un logiciel étant, de toute évidence, occultées, dans leur existence et leurs interactions, aux « yeux » de l'utilisateur final. Dans le second cas, en cas de fonctionnalités divergentes du logiciel initial, il nous semble qu'un tel mécanisme viral puisse être soumis au contrôle du juge en considération des dangers d'un tel outil. Nous remarquerons, à cet égard que lorsque le bénéfice nous semble plus ténu, la notion de consentement nous apparaît nécessaire avec une plus grande force.

Enfin, s'agissant des programmes non désirés, il y a, par nature, une absence de consentement. Dès lors, le bénéfice qui est retiré du virus nous semble devoir être d'une nature « supérieure » et transcender le simple intérêt particulier pour que le virus puisse être considéré comme utile. La notion d'intérêt général vue précédemment réapparaît donc sur ce point.

Ainsi, en fonction du degré de « bénéfice » apporté par le programme d'origine virale, le consentement devra être donné de manière plus ou moins expresse, de manière plus ou moins caractérisée. Une balance des intérêts, opposant « positivité » et « négativité » virale sera donc à réaliser *in concreto*. Afin de préciser la manière dont cette balance va pouvoir mesurer ces intérêts, il nous faut préciser que l'activité du virus ne nous semble pas liée à la notion de fonctionnement optimal du système[152]. Nous pouvons effectivement nous demander, en se fondant sur la coutume, en matière de développement de logiciel, de ne pas considérer comme défectueux un logiciel standard qui n'est disponible sur le système qu'à 98%, si un virus qui consomme d'une manière négligeable les ressources du système peut être considéré comme pouvant porter atteinte au système. En effet, en tant que programme, un virus doit être traité de la même manière que les autres programmes, avec une nuance cependant, compte tenu de son potentiel offensif en matière de mesures de sécurité.

Avant d'analyser plus en profondeur, l'ensemble des mesures nécessaires à l'appréhension globale des virus « bénéfiques » (cf. II/B/2), il nous a semblé intéressant de caractériser les problèmes inhérents aux virus ainsi que leurs caractéristiques essentielles.

3. Caractérisation d'un virus bénéfique

Vesselin Bontchev définit un virus « bon » sur quatre niveaux[153]. Ces quelques considérations ne sont cependant pas partagées par tous, étant précisé que leur nature restrictive ne fait entrer que

[152] TGI Paris, 28 janvier 1993, Comm. Sylvie Rozenfeld, Expertises, avril 1994, p. 127 : le tribunal relaxe les prévenus au motif que le ralentissement des capacités du serveur « *apparaît lié davantage à un fonctionnement optimal du serveu*r [qu'à une véritable nuisance constitutive d'une entrave]».
[153] Vesselin Bontchev, « *Are « good » computer viruses still a bad idea?* », *préc*.

peu d'« infomasse »[154] virale dans le champ des virus bénéfiques. Au vu de ces quatre niveaux, nous allons donc analyser les solutions possibles aux problèmes posés, d'une manière générale, par les virus.

a. Sur le plan technique

Le premier problème soulevé par le phénomène viral est un problème de contrôle : une fois lâché dans une nature virtuelle[155], il devient impossible de prévoir la multiplicité des interactions auxquelles il est partie prenante. Cela pose un réel problème de sécurité car il existera toujours un risque potentiel. Par ailleurs, un virus inoffensif sur un système peut s'avérer extrêmement néfaste sur un autre[156] ; la même idée s'appliquant aux différents format de fichiers : ainsi, un virus de programme fonctionnant par adjonction de code pourrait écraser des données dès lors qu'il infecte un exécutable de données compressées . Afin de remédier à ce problème, il serait, par exemple, possible de lui interdire de sortir d'un système donné ou de lui permettre d'infecter un programme uniquement dans le cas d'une «invitation », d'un accord de l'utilisateur[157] ou d'une authentification du système auprès du virus par un procédé cryptographique.

Le second est un problème de reconnaissance. En effet, au sein d'une multitude de codes nuisibles, il apparaît important de distinguer les programmes viraux « bénéfiques » des autres programmes, de type auto-reproducteur ou non, ne serait-ce que pour faire fi du barrage des logiciels anti-virus. Ces derniers fonctionnent en effet, de manière succincte, selon plusieurs modes : un mode par recherche de signature et un mode générique qui observe les changements des programmes exécutables. Pour solutionner cette difficulté, il semble qu'un virus doive d'une part être doté d'un procédé d'authentification cryptographique fort pour que les éditeurs de logiciels antivirus n'aient pas à inscrire sa signature dans leur base de données antivirale et d'autre part qu'il ne modifie d'aucune manière ces programmes exécutables.

Par ailleurs, comme tout programme, un virus en activité consomme à la fois des ressources en terme de mémoire, de disque dur et de processeur. A ce titre, il convient d'être moins restrictif. En effet, il est impossible qu'un programme ne consomme aucune des ressources du système sur lequel il est installé. Le virus « bénéfique » devra utiliser les ressources du système de manière négligeable que cela soit en tant que tel ou par rapport au bénéfice qu'il apporte à l'utilisateur.

En outre, en tant que programme, un virus peut contenir des « *bugs* ». De par la fonction d'auto-reproduction des virus, ces *bugs* constituent un danger potentiel important. Comme tout programme plus complexe, leurs concepteurs doivent pouvoir d'une part les mettre à jour, d'autre part diffuser ces nouvelles versions de leur virus, ainsi qu'organiser la désactivation de l'ancienne version.

---

[154] Néologisme tiré du terme de biomasse, désignant le poids total de matière vivante sur une surface donnée.
[155] On parle alors de *virus in the wild*.
[156] M. François Paget fait remarquer que le problème viral est toujours lié au système d'exploitation (cf. II/B/1/c)
[157] En 1996 est ainsi apparu le premier virus « poli ». Il demandait à l'utilisateur s'il voulait bien que tels ou tels fichiers soient infectés avant de réaliser cette action.

De plus, se pose un problème de compatibilité, en effet, dans un environnement donné, un virus pourra avoir le comportement attendu, mais dans un autre, une action susceptible de porter atteinte au système. Pour résoudre ce problème, Vesselin Bontchev recommande que les codes viraux ne modifient aucun autre programme mais aussi qu'ils soient indépendants. Il apparaît donc que le programme devra être nécessairement un ver et non un virus (au sens restreint du terme). Nous ajouterons qu'il nous apparaît nécessaire que ces virus/vers ne puissent se reproduire que dans un espace restreint (cf. II/B/2/c).

En dernier lieu, un programme auto-reproducteur, parce que par nature plus dangereux et moins maîtrisable, dans le cadre d'une même tâche, doit pouvoir être plus efficace ou plus rapide qu'un programme plus ordinaire qui ne disposerait pas de cette capacité.

b. Sur le plan éthique

En outre, il ne faut pas nier la possibilité d'utiliser un virus « bénéfique » comme un simple vecteur pour une attaque virale ou humaine, usant du virus comme d'un cheval de Troie et inversant ainsi l'ordre des choses[158]. Cela serait extrêmement néfaste puisque, en ce cas, existerait une certaine confiance dans les mécanismes viraux bénéfiques et donc une absence de protection à leur encontre. Afin d'éviter ceci, il est nécessaire d'identifier et plus précisément d'authentifier, au sens cryptographique du terme, le mécanisme viral de manière certaine afin d'avoir l'assurance de l'absence d'un code malicieux en son sein.

c. Sur le plan juridique

De la même manière que pour toute autre programme, les virus peuvent modifier, de manière non autorisée, certaines données du système. Si dans certaines régions, cela n'est qu'un problème éthique, dans d'autres, comme en France, cela tombe sous le coups des prescriptions pénales (cf. I/B/3). Nous ne pourrons donc considérer un virus comme bénéfique que s'il ne peut modifier ces données, c'est-à-dire que s'il est « invité » sur le système par l'utilisateur de celui-ci et utilise des moyens cryptographiques pour identifier, sans coup férir, la donnée-cible qu'il doit infecter ou modifier, cette cible étant préalablement désignée pour servir de « réceptacle » au virus.

Par ailleurs, modifier un programme ou une donnée soulève une problématique en terme de droit d'auteur. En effet, dès qu'il y a modification du programme, que cette modification s'effectue en terme de code-source ou de code-objet, il y a atteinte aux prérogatives patrimoniales des ayants droits[159]. En outre, nous pouvons ajouter qu'au niveau contractuel, on peut supposer qu'un prestataire informatique refuse de maintenir un logiciel, voire un système au motif, notamment, que l'environnement informatique initial aurait changé du fait de l'infection virale.

Le programme infectieux ne pouvant donc s'adjoindre à un programme hôte, il apparaît nécessaire de disposer d'un outil indépendant et donc un programme de type ver, comme vu précédemment.

---

[158] Robert M. Slade, « *Viral Morality : A Call for Discussion* », 1995 (http://victoria.tc.ca/int-grps/books/techrev/virethic.txt)

[159] Dans la majorité des cas, l'entreprise éditrice du logiciel.

D'autre part, déclarer qu'il puisse exister des virus bénéfiques pourrait amender les concepteurs de virus malicieux qui argueraient alors d'une recherche encore non aboutie ou un essai non concluant ou qui n'a pas eu la destination voulue. Cependant, il n'existe malheureusement pas de solution unique à ce problème. En tout état de cause, un ensemble de mesures doivent être prises ; nous les développerons ultérieurement (cf. II/B).

d. Sur le plan psychologique

Dans un certain sens, agissant de manière autonome et parce que l'ensemble de ses interactions n'est pas connue précisément, le virus « vole » le contrôle du système à celui qui est chargé de la maintenir. Cela peut être la source d'un manque de confiance dans le système de la part des personnes qui en ont la charge. Toutefois, au regard de la complexité des logiciels actuels, ce contrôle n'est qu'une illusion, illusion que les virus peuvent maintenir par les voies énoncées précédemment, à savoir l'usage de la cryptographie asymétrique, à des fins d'authentification.

Partant de ceci, Vesselin Bontchev présente quelques exemples de « virus bénéfiques »[160] : un virus de mise à jour automatique du système d'exploitation, celui de mise à jour centralisée des anti-virus, ainsi que le ver *Xerox* PARC[161].

Après avoir déterminé les mesures techniques et juridiques dans lesquelles un virus bénéfique pourrait exister et se diffuser, il convient d'examiner les mesures qui pourraient être mises en place afin qu'ils puissent devenir des outils informatiques à part entière.

[160] Au vu de sa définition quelque peu restrictive, il ne classe pas dans cette définition les concepts de virus antivirus, de virus compresseur, de virus encrypteur ainsi que de virus de maintenance. D'autres auteurs les classent pourtant dans les virus « bénéfiques ». Nous observerons que peut se surajouter aux problèmes posés par le mécanisme auto-reproducteur d'autres désagréments tels que celui de la diffusion massive d'un correctif ou d'une mise à jour défectueuse.

[161] Ver programmé initialement pour permettre d'utiliser les ressources des systèmes inactifs.

Section B - Prospectives pour une « vie » juridique des infections bénéfiques

La consécration des virus informatiques en tant que véritable outil informatique nous semble reposer sur deux composantes : d'une part la protection contre le pendant négatif de ces virus (1) et d'autre part une reconnaissance à part entière (2)

1. La lutte contre les infections informatiques « négatives »

Cette lutte s'inscrit nécessairement dans le temps. A ce titre, il est nécessaire d'appréhender les futurs mécanismes viraux (a) avant de s'attarder sur les mécanismes en eux-mêmes, en distinguant les mécanismes *a priori* (b) des mécanismes *a posteriori* (c).

a. Virus et évolution

Depuis leur apparition, les virus informatiques ont beaucoup évolués. Ils sont aujourd'hui communicants, dotés de la capacité de se mettre à jour par eux-mêmes et présents sur toutes les plate-formes. Cependant, à l'instar d'un organisme biologique, et par la main de leur concepteur, ils évoluent encore. Pour M. François Paget, la menace virale de demain évoluera dans le sens d'une « *association d'un suffixe @mm*[162] *avec l'exploitation d'une vulnérabil*ité » ce qui, compte tenu de l'augmentation en absolu des connections permanente à Internet permettant une diffusion et, par conséquent, une prolifération plus rapide, nous paraît particulièrement fondé[163].

Dans un texte de 2000[164], Michal Zaleski, un « *hacker* » polonais donne les grandes lignes du développement d'une nouvelle génération de virus. Il exprime ainsi que le virus (un ver plus exactement), doit être portable sur n'importe quel système d'exploitation, doit rester indétectable le plus longtemps possible et être capable d'intercepter les demandes de contrôle émanant de l'antivirus ou du système d'exploitation, s'auto-répliquer ou s'auto-exécuter sans interaction utilisateur, en utilisant sa propre base d'exploits qu'il doit être capable d'améliorer[165]. Par ailleurs, pour être indétectable, il doit être totalement polymorphe, ne disposant d'aucune portion de code constante d'une exécution à une autre, doit être capable de réaliser des objectifs, de télécharger des instructions et de disparaître une fois sa mission terminée et, enfin, sa structure comme celle du protocole *Wormnet* doit être difficile à décoder. Il s'avère que le ver ne serait plus isolé, mais

---

[162] Par "@mm", il faut comprendre un mécanisme qui possède un processus opérationnel de propagation multiple par messagerie électronique ; à la différence du suffixe « @m » qui désigne les mécanismes qui possèdent un processus opérationnel de propagation par messagerie électronique mais qui ne ciblent qu'une seule boite à lettres à chacune de leur activation

[163] Nous ajouterons que, techniquement, la rapidité de propagation est moins liée à la rapidité du réseau ou à la taille du programme qu'à d'autres facteurs relatifs aux nombres de connexions, leur durée ou les principes même du réseau (le ver *Slammer/Blaster* n'était composé que de 316 octets et utilisant un port UDP, il n'était contenu que dans un seul paquet !)

[164] Michal Zaleski,, « "*I don't think I really love you" or writing internet worms for fun and profit* », 2000 ; (http://www.tla.ch/TLA/NEWS/2000sec/20000512Zalewski.htm). Plus exactement, il utilise les termes de : portabilité, invisibilité, indépendance, intelligence, intégrité, polymorphisme, rentabilité.

[165] Il introduit ainsi l'idée du protocole Wormnet, un canal spécial de communication permettant, entre autres la mise à jour des vers. L'idée est d'utiliser un système sain pour infecter les autres. Il existerait une *Virus Communication Interface*, qui utiliserait les processus de communication de son hôte pour communiquer avec des virus modulaires.

plutôt lié à une structure déjà existante : un protocole de communication chargé, entre autres, de lui permettre de s'améliorer[166].

Autre exemple : le réseau *Sinit*[167]. *Sinit* serait un réseau *peer-to-peer* privé, créé afin de diffuser virus, vers et autres codes malicieux. Utilisant un réseau *peer-to-peer*, la diffusion s'effectuerait donc sans serveur central dont on pourrait demander l'arrêt. Chaque hôte infecté devient un élément de ce réseau à travers lequel d'autres chevaux de Troie peuvent être diffusés à tous les autres serveurs hôtes. *Sinit* permettrait une dispersion rapide des virus et utiliserait une technologie de cryptage sophistiquée pour empêcher les éditeurs d'anti-virus de pister l'activité de développement ou de modifier les codes viraux. Il pourrait aussi constituer la plate-forme de lancement d'un futur "super-ver" extrêmement efficace.

Quelle que soit la réalité de ces projets, une nouvelle idée a fait son chemin. Les virus ne sont plus créés de manière isolée, ils sont l'objet de projets à long terme visant non plus le simple défi intellectuel ou cyberdélinquance mais le profit financier[168]. A ce titre, la convergence entre les différentes cybercriminalités (virus, courriers électroniques non sollicités, intrusions, …) est bien réelle rendant la protection encore plus nécessaire et complète.

b. Les mécanismes de lutte antivirale *a priori*

Il s'agit des mécanismes de lutte mis en place avant l'infection même. On trouve au premier rang de ceux-ci, bien évidemment les logiciels antivirus.

- Les logiciels antivirus

La lutte contre les virus passe nécessairement par ce type de logiciels. Participant à une sorte de sélection informatique des organismes logiques qui laisserait opérer, de fait, ceux qui se diffusent peu, il s'agit des seuls susceptibles de nettoyer un espace mémoire de ses programmes nuisibles de manière automatique. Il convient toutefois de préciser qu'un simple logiciel ne suffit pas, qu'il est impératif de le mettre à jour mais aussi qu'il fonctionne de manière statique et dynamique. Dans le premier cas, en faisant appel à des techniques de recherche de signature, d'analyse spectrale, heuristique[169] ou tout simplement de contrôle d'intégrité, l'antivirus est n'actif qu'à la demande de l'utilisateur du système ; dans le second, via des analyses de comportements de programmes et d'émulation de code, [170]il réside dans le système et le surveille, ayant priorité sur

[166] Marc Blanchard, *« Les prochains développements sur les codes malicieux : Rêves de hackers ou réalité ? »,* Conférence présentée au salon de la sécurité informatique au CNIT La Défense (2001).

[167] Nous noterons que son existence même est contestée. Pour certains, il s'agit d'une simple manœuvre de désinformation (F. Paget).

[168] Bien que le crime organisé domine en partie la scène du code malicieux, les groupes de création de virus traditionnels (29a, 40Hex…) sont toujours actifs. Sérotonin (2003), non diffusé, inaugure ainsi une nouvelle génération de vers utilisant des techniques de "programmation génétique" pour imiter les mécanismes de sélection naturelle. Il représente un bon exemple des problèmes à venir.

[169] La recherche de signature va rechercher une suite d'éléments logiques caractéristiques du virus, l'analyse spectrale va analyser les programmes et repérer les séries d'instructions peu courantes et l'analyse heuristique va détecter les actions potentiellement virales.

[170] Le code de chaque programme scanné par le logiciel antivirus va être étudié dans une zone mémoire confinée puis est émulé afin de détecter un comportement potentiellement viral.

celui-ci en cas de présomption d'attaque virale du système[171]. Ceci n'est toutefois pas suffisant et une réelle politique de sécurité informatique doit souvent être mis en place.

- La mise en place d'une politique de sécurité réfléchie

Un simple logiciel antivirus ne suffit effectivement pas. Il est nécessaire de prévenir les risques viraux sur d'autres plans, via une véritable politique de veille technologique, et notamment par rapport aux utilisateurs eux-mêmes. En effet, ces derniers, par curiosité ou par manque d'information ou de formation, représentent véritablement le premier vecteur de transmission des mécanismes viraux nuisibles. Aux fins de résoudre ce problème, il apparaît que la rédaction d'une charte relative à l'utilisation de l'informatique dans une entreprise ou que l'envoi par un prestataire technique[172] d'une notice dans le cas d'un particulier est une nécessité impérieuse et primordiale.

Par ailleurs, l'installation des correctifs et mises à jour de sécurité, l'instauration de droits limités sont, elles aussi, nécessaires. En effet, l'éradication des virus passe, non pas par une protection *a priori*, mais pas un système qui rend impossible, techniquement ou socialement, leur diffusion ; un virus spécifique à un système ou à une entreprise établi à des fins d'espionnage informatique étant transparent à l'heure actuelle pour la majorité des logiciels antivirus (les méthodes d'analyses par recherche de signatures s'averrant au final inefficace).

Nous pouvons toutefois nous poser la question de la multiplication de ces correctifs. Il en est créé plusieurs dizaines par jour pour certains logiciels et cela pose au surplus de nombreux problèmes de compatibilité et de « *bugs* »[173]. Ne pourrait-on pas imaginer, par exemple, un langage de programmation pensé pour rendre impossible les bogues logiciels et donc, par conséquent, rendant inutile la diffusion de correctifs dont la plupart ne sont jamais appliqués. Il est vrai qu'un tel logiciel, de par les routines de vérification qui lui seraient inhérentes, serait relativement gros consommateur de ressources, mais, par ailleurs, le temps gagné pourrait permettre une meilleure optimisation du logiciel et donc une consommation moindre de ces même ressources[174].

Il reste néanmoins des problèmes contre lesquels aucun logiciel ou aucune politique de sécurité ne saurait agir. C'est notamment le cas des accès dissimulés pour lesquels la seule solution serait de repartir avec un système neutre, c'est-à-dire vierge[175].

---

[171] Un bon exemple est le logiciel *PrevX* (http://www.prvx.com).

[172] L'éditeur de logiciel antivirus est, à ce titre, le mieux placer pour informer les particuliers dans le cadre de l'achat d'un de leur logiciel.

[173] Nous pouvons citer l'exemple de la société IBM qui, lors de la sortie du *Service Pack 2* pour le système d'exploitation *Windows* XP, a procédé elle-même à des tests de compatibilité avant d'autoriser son personnel à procéder à la mise à jour : http://www.pcinpact.com/actu/news/Message_integral_du_message_dIBM_a_propos_de_SP2.htm.

[174] Corrélativement, cela pose le problème de l'opportunité de la protection des langages de programmation par le droit d'auteur.

[175] A moins, bien sûr, de réaliser son propre microcode, système d'exploitation, compilateurs et utilitaires, rien ne nous permettant d'être sûrs qu'une application donnée même si les sources en sont disponibles ne recèlera pas un tel accès.

- Le monopole des logiciels propriétaires comme vecteur de diffusion des virus

Bien que cela ne soit pas réellement un mécanisme de lutte contre les virus nuisibles, cela participe grandement à leur action. En effet, les virus actuels n'étant pas majoritairement multi-plate-formes, le fait que 93,8% des systèmes particuliers et 55,1 % des systèmes professionnels fonctionnent grâce à un système d'exploitation propriétaire de type *Windows*[176] est une des clés de leur succès, l'homogénéité des parcs informatiques provoquant, à titre accessoire, celle des failles de sécurité et ce quelque soit le système d'exploitation en cause.

Ainsi, partant du postulat que dans les systèmes exclusifs, les utilisateurs s'échangent de proche en proche des programmes, alors que dans les systèmes libres, ils vont directement chercher les logiciels à une source sûre[177], François-René Rideau explique comment les logiciels propriétaires favoriseraient l'émergence des virus informatique. Dès lors, le monopole portant sur un logiciel serait un facteur aggravant de cette émergence[178], mais il semble que l'exclusivité soit elle-même un facteur aggravant supplémentaire.

En effet, les éditeurs de logiciels exclusifs interdisent de copier et de rediffuser légalement leurs programmes. S'il s'agit de programmes gratuits, ils se réservent souvent le monopole de la diffusion de leurs logiciels à travers une procédure contraignante (enregistrement en ligne, envoi du support postérieur à l'achat, etc). Par ailleurs, il existe de très nombreux outils destinés à pallier leurs déficiences en terme de fonctionnalités qui sont disponibles selon des sources très diverses et développés sans concertation aucune. Il en découlerait une certaine « promiscuité du logiciel », favorable aux infections virales, qu'il s'agisse de copies licites ou non.

En outre, dans de nombreux logiciels exclusifs, afin de faciliter la « modularité » des programmes, existent des mécanismes d'exécution implicite de code (documents *Office*, pages Internet, messages de courrier électronique, fichiers .zip, de répertoires, etc). Cela aurait ouvert la voie a un très grand nombre de programmes viraux, qui tirent parti de telles fonctionnalités pour s'activer à l'insu de l'utilisateur, qui croit consulter un document inoffensif.

D'autre part, en matière de logiciels exclusifs, les délais de correction, par rapport à un système libre de type BSD ou *Linux*, sont souvent plus longs, le monopole étant plus fort sur certains segments du marché et provoquant une sorte de captivité des clients n'enjoignant pas la fourniture rapide d'un correctif et non favorable à la concurrence. Ceci est à lier avec le

---

[176] Selon le cabinet d'étude IDC, en 2002, les parts de marché des systèmes d'exploitation se divisaient comme : pour les serveurs : *Microsoft Windows* (55,1%), *Linux* (23,1%), *Unix* propriétaires [notamment AIX pour IBM ; HP-UX pour *HP-Compaq* ; *Solaris* pour *Sun* avant l'ouverture de son code, IRIX pour SGI, *Xenix* pour *Microsoft*, xBSD …] (11,0%), *Novell Netware* (9,9%) ; et comme suit pour les postes clients : *Microsoft Windows* (93,8%), *MacOS* (2,9%), *Linux* (2,8%). Selon le cabinet *Gertner*, la part de marché de *Linux* serait passée à 3,2 % sur ces derniers, en majorité au détriment des systèmes *Unix* (http://www.logiciellibre.net/2004/shortnews20040330.php). Ces données sont à prendre avec circonspection. D'autres études sont en effet susceptibles de les infirmer.

[177] François-René Rideau, « *Les virus informatiques comme sous-produits des logiciels exclusifs* », article essentiellement écrit entre le 2001-07-31 et le 2001-08-01, disponible sous licence *Bugroff*.

[178] Dans sa démonstration, il cite bien évidemment le système *Windows* mais généralise à l'ensemble des logiciels propriétaires, les arguments développés étant essentiellement liés au mode de diffusion de ces logiciels.

cloisonnement des formats provoquant une sorte de vulnérabilité automatique et forcée des systèmes[179].

Au surplus, les éditeurs de logiciels exclusifs, fournissant un binaire précompilé plutôt que leurs sources, doivent assurer la rétro-compatibilité de leurs logiciels, ce qui provoquerait une certaine inertie à l'évolution de ces même logiciels aboutissant souvent à une obsolescence occultée et une incompréhension technique et globale de certaines parties du système. En effet, la multiplication des correctifs au sein d'un logiciel n'a pas pour conséquence de permettre une meilleure lisibilité de son code, ce qui apparaît être pourtant un moteur de son évolution et une source de sécurité.

En tant que corollaire du postulat précédent, il serait très difficile de tracer la diffusion d'un logiciel, et par là même celle d'un virus se propageant à travers ce logiciel, mais aussi d'auditer le code, afin de voir s'il contient effectivement un code malicieux.

Ces quelques arguments en faveur, d'une part, de l'hétérogénéité des systèmes d'informations[180] et, d'autre part, en faveur des systèmes dits « libres » peuvent être catégorisés en deux ensembles : en premier lieu, les monopoles de propriété intellectuelle propres au modèle exclusif, qui, en rendant illégale toute tentative d'organisation efficace et centralisée de la diffusion des logiciels, créent une situation d'inefficacité légalement obligatoire et favorisent les attaques des virus ; en second lieu, ils créent une dynamique anticoncurrentielle nuisible à la qualité de développement et la transparence des logiciels[181]. Ces deux facteurs tendent, pour nous, par conséquent, à faire de la lutte antivirale post-infection, un mécanisme de régulation alors qu'elle ne devrait être qu'un mécanisme de réparation.

D'autres sources amènent toutefois des arguments contraires. Ainsi, la société *Secunia* compare les vulnérabilités d'un système d'exploitation propriétaire et d'un autre, libre[182]. Les résultats sont, comme on pouvait s'y attendre, plus mitigés. Les systèmes pris en référence disposent en effet d'atributs en matière de sécurité qui leur sont propres, lesquels deviennent difficiles à comparer. Pour ne prendre qu'un exemple, le système *RedHat* dispose de plus de failles, mais les voit toutes résolues, au contraire d'un système *Microsoft* (selon cette étude) pour lequel il reste quelques éléments non corrigés.

c. Les mécanismes de lutte antivirale *a posteriori*

Il s'agira ici d'analyser succinctement les mécanismes de responsabilité, ainsi que le système de l'assurance.

---

[179] D'une manière générale, un document *Word* va être ouvert par le programme *Word*. En dehors des visionneuses, il n'existe effectivement pas d'autres programmes permettant ceci.

[180] L'hétérogénéité ne doit pas être comprise comme une anti-intéropérabilité mais comme un palliatif aux défauts des systèmes d'exploitation actuels qui privilégient la compatibilité à la sécurité.

[181] Il s'agit là des résultats d'une bonne partie des études portant sur la distinction logiciels propriétaires/logiciels libres bien qu'il en existe quelques-unes qui soient dissidentes (étude de *Forrester Research* « *Is Linux More Secure than Windows ?* » rapportée dans Le Monde Informatique par Olivier Rafal, 16 avril 2004, N°1022, p.6 ; le texte de l'étude peut être trouvé en suivant : http://www.microsoft.com/windowsserversystem/facts/analyses/default.mspx#EHA).

[182] Voir les liens : http://secunia.com/product/2535/ et http://secunia.com/product/1174/.

- L'assurance : un échec relatif

Si les assurances offrant des garanties contre les virus existent depuis la fin des années 1980, elles ne semblent toutefois pas avoir proliférer. En effet, en matière d'assurance, afin de pouvoir se voir rembourser un dommage, il faut prouver qu'il y a eu un dommage, causé par un élément prévu au contrat d'assurance. Or, un problème majeur se pose. De manière accessoire, un virus peut endommager du matériel, mais l'atteinte principale qu'il peut produire se trouve au sein des données. Or, s'il est facile de quantifier un dommage sur du matériel, effectuer la même opération sur des biens immatériels comme une simple information est beaucoup plus difficile. Tout au plus peut-on considérer le dommage comme l'ensemble des frais engagés dans le but de recouvrer ces informations ainsi que ceux subséquents (perte d'activité, de confiance, …) lesquels peuvent être très difficiles à évaluer.

Par ailleurs, la question de la preuve est aussi délicate. En effet, la destruction d'une donnée peut avoir plusieurs sources et notamment virale, sans que l'on puisse dire de manière précise quel est le fait générateur de la destruction.

En matière de responsabilité civile, Pascal Lointier[183], président du CLUSIF, fait remarqué que la plupart des contrats d'assurance responsabilité civile exclut expressément le remboursement des dégâts consécutifs à un virus informatique notamment en considération du risque sériel, c'est-à-dire le cumul du nombre de plaintes ou d'appels en garantie en cas de découverte d'une entreprise qui aurait contribué à propager le virus par exemple, mais aussi en raison de la peur d'un virus à propagation rapide touchant un nombre très important de personnes.

- La responsabilité civile délictuelle.

Par ailleurs, la question de la responsabilité civile délictuelle pourrait être soulevée. Le droit commun de la responsabilité civile délictuelle, fondé sur l'article 1382 du Code civil, rend nécessaire que soit prouvée une faute, un dommage et un lien de causalité entre les deux. La faute consiste ici en la conception ou la diffusion d'un mécanisme offensif[184]. Le dommage, quant à lui peut être de nature très diverse : perte de données, de disponibilité du système, etc. Enfin, le lien de causalité entre la faute et le dommage doit être clairement établi. Ainsi, il ne subsiste aucun doute quand à la caractérisation de ces trois éléments en cas d'entente entre les auteurs de virus et les éditeurs de logiciel antivirus[185].
En matière de virus, il nous apparaît évident que cela soulève un problème de compétence judiciaire, le virus étant conçu ou diffusé, le plus souvent, de l'étranger. Succinctement, en droit français, le tribunal compétent pour juger un litige international est, en principe, celui du domicile

[183] Pascal Lointier, « *L'assurance contre les virus informatiques* », MISC, n°5 (2003)
[184] ADBS, *Actualités du droit de l'information*, « *Liste de diffusion* » N°29, octobre 2002, p. 3 : L'expéditeur du virus est responsable de l'infection et des dommages causés s'il le transmet volontairement. Cependant, si la transmission est involontaire, son comportement sera évalué et sa responsabilité sera engagée s'il a négligé de prendre les mesures de prudence élémentaires.
[185] Danielle Kaminski, étude pour le compte du CLUSIF : « *Auteurs de virus, Entreprises, Editeurs d'antivirus : les liaisons dangereuses* » (octobre 1998) ; commenté par Sylvie Rozenfeld, « *Responsabilité des éditeurs d'antivirus* », Expertises, novembre 1998, p. 328.

du défendeur, à moins que le demandeur, s'il est français, ne souhaite invoquer le privilège de juridiction des articles 14 et 15 du Code civil. Or, ce dernier privilège est interdit dans le cadre de la Communauté européenne par la Convention de Bruxelles de 1973, devenue en 2000 un règlement " *concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale* ".

Dans le cas où le dommage causé par le virus serait survenu au sein du système informatique d'une société domiciliée en France, les juridictions françaises seraient sans doute compétentes pour juger le litige.

Quant à la loi applicable, le juge applique, de manière générale, la *lex loci delicti*, c'est-à-dire la loi où le fait dommageable s'est produit. La Cour de Cassation a jugé que le lieu où le fait dommageable s'est produit « *s'entend aussi bien de celui du fait générateur du dommage que du lieu de réalisation de ce dernier* »[186].

- La responsabilité civile contractuelle.

Par ailleurs, il serait envisageable d'engager la responsabilité civile contractuelle de l'éditeur d'antivirus. En effet, la défaillance du logiciel antivirus devrait permettre de se voir réparer les dommages consécutifs à cette défaillance.

Cependant, cette responsabilité rencontre des difficultés de mise en œuvre. En dehors de la nécessité de procéder à la mise à jour des bases de signatures virales et du logiciel lui même de manière régulière, les éditeurs spécifient toutefois quels sont les virus susceptibles d'être éradiqués par leur logiciel. Il nous faudrait donc examiner les clauses contenues dans le contrat de licence et s'apercevoir que les éditeurs sont liés par une obligation de moyen quant à l'éradication des virus informatiques, ce qui, compte tenu de l'évolutivité de la matière, apparaît raisonnable. L'éditeur ne sera donc contraint que d'apporter la preuve qu'il n'a pas manqué aux obligations normales qui lui incombaient.

D'autres responsabilités pourraient être recherchées, comme celle du fabricant du support physique de données incluant un virus, en vertu de la garantie des vices cachés de l'article 1641 du Code Civil[187], celle du fournisseur de virus, en vertu de la responsabilité du fait des produits défectueux des articles 1386-1 à 1386-18 du Code Civil, mais leurs implications nous semblent tellement minimes que cela ne peut influer sur le devenir des virus « néfastes » que de manière négligeable.

La solution serait donc, non pas de les éradiquer *a posteriori* comme pourrait le faire un anti-virus, mais de procéder à cette élimination de manière préventive, *a priori*. En effet, en se fondant sur une analyse *a posteriori*, une partie du mal est déjà réalisée : un certain nombre

[186] Cass. 1re civ., 14 janvier 1997, D. 1997, p.177

[187] Cass. Com., 25 novembre 1997, Aff. Exa Publications : l'éditeur qui vend une revue dans laquelle est insérée une disquette infectée par un virus est tenu de réparer les dommages causés par la disquette sur le fondement de la garantie des vices cachés. Voir aussi : CA Versailles, 4 octobre 2002 : la réparation des vices rendant la chose impropre à son usage empêche l'action en garantie des vices cachés.

d'infection a déjà eu lieu et, dans une certaine mesure, la propagation a commencé. Seule la propagation « critique » est bloquée (excepté en cas d'antivirus générique).

2. Propositions pour une prise en compte juridique des virus informatiques

En considération des éléments précédents, un certain nombre de mesures ont été prises pour lutter contre les virus nuisibles. Dès lors, il convient d'étudier les pistes conduisant à l'appréhension économique des virus bénéfiques.

a. Changement de dénomination informatique

Il nous apparaît évident que la première chose à envisager afin de favoriser cette appréhension est le changement de dénomination de ces virus bénéfiques. En effet, la proximité sémantique avec les virus nuisibles ne peut que les desservir.

A ce titre, en continuant de se baser sur la distinction du code auto-reproducteur de la charge finale, il pourrait convenir de les nommer « programmes auto-répliquants ». En effet, par ce choix lexical, la connotation délictuelle de nuisance disparaît au profit d'une notion informatique et technique mettant en avant leur capacité à se dupliquer. Il convient de préciser que nous préférons le terme de « réplique » à celui de « reproduction » car la notion de duplication « asexuée » est plus présente (les virus binaires, de par leur rareté, ne sont effectivement pas significatifs). De même, elle fait plus état d'une duplication à l'identique avec certains éléments changeants, ce qui nous paraît plus conforme aux mécanismes viraux ; rappelons que le polymorphisme modifie seulement la « forme » du code et non le « fond ». Dès lors, par cette nouvelle dénomination, il n'apparaît plus de manière aussi définitive que l'on doive considérer les virus comme des nuisances par nature et organiser une certaine forme de psychose dès l'apparition de l'un d'entre eux sur l'Internet.

b. Proposition de dispositions légales

En l'état actuel de la loi, il nous semble nécessaire de la réformer dans une certaine mesure. En effet, si elle appréhende la technique de manière neutre, il conviendrait d'en réduire le champ d'application. Ainsi, pour nous, l'article L.323-2 du Code Pénal pourrait subordonner le « faussement » d'un système à une condition de gravité, par exemple par l'ajout de l'expression « de manière grave ou évidente ». Cela aurait pour effet, effectivement, de ne plus appréhender certains mécanismes comme les virus espions mais, toute chose égale par ailleurs, ces derniers tombent sous le coup d'autres textes comme ceux relatifs à la protection de la vie privée mais cela permettrait aussi de ne plus pouvoir appréhender pénalement le moindre auteur d'un logiciel ne consommant que peu de ressources du système et ne portant pas atteinte aux droits de l'utilisateur légitime. Des mécanismes autres que pénaux sont disponibles pour régler ces situations et sont, à notre avis, plus intéressants à mettre en œuvre que cette épée de Damoclès pénale.
En outre, il conviendrait de prévoir à l'article L.323-3-1 du Code Pénal une exception d'utilisation à des fins de recherche réglementée par un système d'autorisation préalable auprès d'un organisme agréé. Cela aurait pour conséquence d'identifier de manière certaine les

organismes, personnes physiques ou morales, capables d'étudier ces mécanismes, étant entendu que, dans le cadre de cette recherche, de nombreuses mesures de sécurité devront être mises en place afin que l'incident de l'Internet *Worm* ne puisse se reproduire.

Nous préférons un système d'autorisation à un système de déclaration préalable, eu égard au fait que l'autorité chargée de cette mission devra adopter un comportement actif et non, comme dans le cas d'une simple déclaration, un comportement passif pouvant entraîner des erreurs quant aux personnes habilitées à procéder au développement de tels codes, erreurs qui pourraient s'avérer préjudiciables dans le futur[188]. Eu égard à la matière, cette réactivité nous apparaît indispensable.

c. Une nouvelle notion : l'espace confiné

Une des séries de mesures les plus importantes à mettre en place afin de permettre la mise en œuvre des virus bénéfiques est celle relative à l'isolement de ceux-ci des secteurs des systèmes d'information où il n'est pas expressément nécessaire, étant précisé que ces systèmes peuvent être de toute nature, du simple ordinateur de bureau à l'Internet. Ceci nous semble indispensable afin de ne pas encombrer de virus inutiles les systèmes d'information actuels et donc optimiser le rapport coût/bénéfice de tels programmes. En effet, il est probable qu'une fois ce domaine entré dans le champ économique, chaque entreprise développe son propre programme viral afin, par exemple, d'automatiser certaines tâches. Dès lors, le risque serait la paralysie des systèmes par saturation des réseaux et des capacités de calculs de ces systèmes.

Partant de ce constat, et par analogie avec les laboratoires de recherche en virologie biologique, il convient de confiner les virus, tant au niveau du développement que lors de son exploitation, à un système ou un ensemble de système directement maîtrisés ou directement maîtrisables. De la même manière que les virus sont étudiés dans des salles sous-pressurisées afin qu'ils ne puissent se propager à l'extérieur en cas de problème majeur, le virus pourrait contenir une portion de code ne lui permettant pas de sortir du système auquel il est lié[189].

d. La mise en place d'un système de certification

Afin de pouvoir exploiter de manière économique les mécanismes viraux, il conviendrait de mettre en place un système de certification chargé d'auditer, d'autoriser et de suivre la diffusion de ces mécanismes. De manière optimale, ce système devra être mis en place au niveau international ou au niveau national mais, en ce cas, avec la création d'un organisme centralisateur chargé d'harmoniser les certificats mais aussi d'établir des recommandations techniques en matière de développement de tels mécanismes.
Ces certificats pourraient n'être ainsi délivrés que si le virus répond aux conditions d'intégrité et de contrôle, telles que définies par Vesselin Bontchev et, notamment, afin de ne pas encombrer

[188] Il est aussi vrai que des abus seront possibles dans le cas de la déclaration préalable : « administrativisation » des procédures, délais, …
[189] De manière très simple, le virus pourrait être lié aux adresses IP ou MAC des serveurs d'une société, à un unique serveur en grappe (*cluster*) ou soumis à la présence d'un code autorisant sa diffusion ainsi que les cibles de la diffusion sur un serveur distant.

inutilement les réseaux et les systèmes de portions de code « mort », s'il contient les éléments de programmation nécessaires à sa disparition sans dommage pour le système hôte.

La solution envisagée se rapproche de celle déjà existante en matière de cryptographie. Le choix n'est pas innocent. En effet, la diffusion non dommageable d'un virus repose, pour une bonne partie, sur une maîtrise des procédés de cryptographie qui leur permettrait de s'assurer du respect des conditions d'exploitation de tels mécanismes viraux, comme vues précédemment. Par ailleurs, nous ne connaissons pas d'autres procédés permettant d'aboutir au même résultat qu'un cryptosystème à clés publiques avec la même simplicité de mise en œuvre.

e. L'établissement de véritables programmes de recherche

Au regard des résultats des expériences menées par Fred Cohen en novembre 1983, juillet et août 1984[190], nous pouvons observer la réticence existante alors à étudier un mécanisme au potentiel offensif important. Il nous semble que cette réticence est encore d'actualité. Il nous faudra cependant la vaincre afin d'effectuer de véritables percées scientifiques en ce domaine, via des programmes de recherche menés conjointement par les organismes publics et privés. Cependant, les mentalités commencent à évoluer et cette dernière année a vu naître aux Etats-Unis un projet de système informatique isolé afin d'étudier les implications en matière de défense des mécanismes viraux[191]. Il n'y a, dès lors, que quelques pas à franchir pour que l'on puisse utiliser un virus comme un outil informatique standard : celui de l'intérêt économique, mais surtout celui de la volonté. En effet, nous ne pouvons citer pour illustrer ceci que le fait que, dans les années 1980, il a été offert, à titre gracieux, à *Microsoft* et IBM, une technique qui empêchait toute infection du secteur de « *boot* » des périphériques de stockage, technique qui a été malheureusement refusée.

[190] Eric Filiol, op. cit. *supra* pp.58-60.

[191] Une équipe de chercheurs issus des universités de Californie du Sud et de Berkeley a reçu une subvention de 5,46 millions de dollars pour créer un simulateur d'Internet. Le projet *Cyber Defense Technology Experimental Research Network* (ou projet DETER) a pour but de pouvoir apprendre à parer les attaques logiques de type saturation ou virus. Les "faux réseaux" existants étaient beaucoup trop petits (une douzaine de machines au plus) pour tenter de véritables expériences reproduisant un comportement semblable à celui de l'Internet. il fallait donc passer à la taille supérieure~ en l'occurrence un millier d'ordinateurs (Bertrand Lemaire, *Ersatz : Internet simulé dans des réseaux fermés*, Le Monde Informatique, 23 janvier 2004, n°1010, p.42).

Conclusion

Internet n'a initialement pas été conçu pour un emploi civil. En effet, il est issu de l'Arpanet, réseau utilisé à des fins de défense par les Etats-Unis à partir de 1974 et en adopte donc les éléments essentiels. Ainsi, par conséquent, les qualités, mais aussi les défauts du premier, vont se retrouver, d'une manière générale, dans le second (par exemple le problème de l'authentification des expéditeurs de courriels via le protocole SMTP).

A ce titre, il n'a pas été conçu pour une utilisation massive par un ensemble en grande majorité néophyte. Il apparaît donc normal qu'il révèle, dans le cadre de cette utilisation, des limites inconnues à l'origine. Une de ces limites est la propagation et la prolifération des virus, véritable fléau mais aussi, comme nous avons chercher à le démontrer, un outil potentiel véritablement puissant devant s'inscrire, en considération des dérives actuelles, dans des règles de mise en œuvre très strictes.

Il est certain cependant que les mécanismes viraux utiles pourraient apporter une réelle dynamique à l'industrie informatique, apportant une technique et un mode de pensée légèrement différent de celles et ceux qui existent actuellement.

Cependant encore faut-il en accepter le concept et prendre les mesures adéquates en ce sens. Ceci ne paraît pas si aisé et l'on risque d'aller vers une situation à deux vitesses, comme souvent en informatique, entre ceux qui « savent » et les autres, les néophytes, la majorité, qu'il faudra pourtant informer et éduquer en matière de sécurité informatique, car la sécurité des systèmes d'information demeure entre leurs mains. En effet, le virus constitue un danger informatique de nature structurelle et non conjoncturelle, et seule une refonte complète de ces systèmes d'information pourrait véritablement les annihiler.

Remerciements

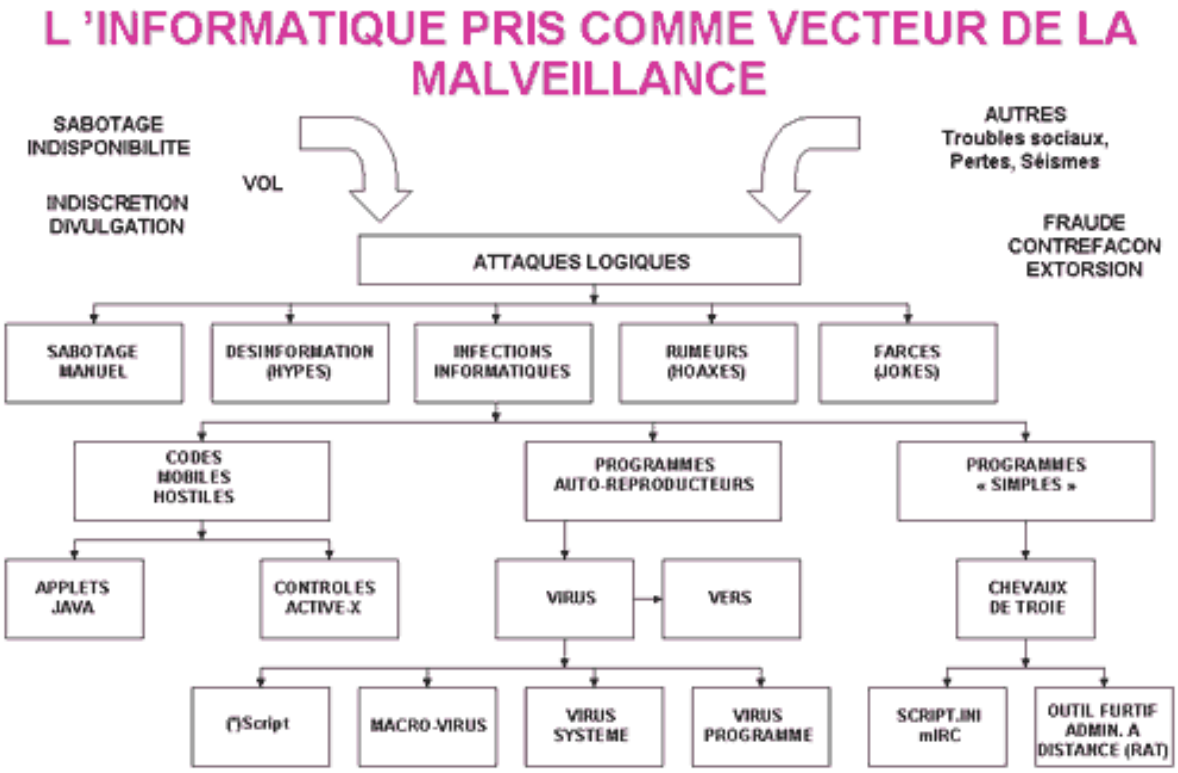
Je tiens à remercier tout particulièrement ceux qui m'ont aidé à faire ce mémoire :

Maître Olivier Iteanu, Mme Corinne Moizan, M. Eric Filiol, M.François Paget ;

Ainsi que l'ensembles des personnes qui ont participé à la recherche documentaire : le DESS D2NT (et particulièrement Mlle Vera Lukic) et la mailing-list alt.comp.virus.

ANNEXES

Annexe 1 : Tableau récapitulatif des infections informatiques



Source : http://www.perso.wanadoo.fr/malware.fr

Annexe 2 : Le Virus Informatique : première forme de vie logique ?

Quelques éléments supplémentaires sur cette question :

1. Le biologiste J. de Rosnay distingue quatre fonctions fondamentales chez les êtres vivants[192] :
   - l'auto-conservation, qui est la capacité à se maintenir en vie par la nutrition ;
   - l'assimilation et les réactions énergétiques de la respiration et de la fermentation ;
   - l'auto-reproduction, qui est la capacité de propager la vie ;
   - l'autorégulation, qui est la capacité de se gérer soi-même par la régulation et le contrôle.

2. Par ailleurs, lors de la seconde conférence *Artificial Life*, J.D. Farmer et A. Belin ont présenté une liste de critères déterminant si un être, naturel ou artificiel, peut être considéré comme vivant ou non :
« *La vie est une structure dans l'espace-temps, plutôt qu'un objet matériel spécifique, signifiant que l'organisation de l'être vivant est plus importante que l'identité spécifique des éléments qui la composent.*
La vie implique un mécanisme d'auto-reproduction, direct ou indirect au travers d'autres organismes, comme dans le cas des virus.
Un être vivant comprend une description de lui-même qu'il utilise pour se reproduire, stockée sous forme de chaînes d'acides nucléiques dans les chromosomes des cellules.
Un être vivant possède un métabolisme qui convertit la matière ou l'énergie de l'environnement dans les formes et les fonctions utiles à l'organisme.
Un être vivant interagit fonctionnellement avec son environnement, il est capable de répondre à des stimuli perçus, et d'effectuer des actions sur son environnement en fonction de ses perceptions.
Un être vivant est composé d'un ensemble de structures interdépendantes qui constituent son identité. Si l'on altère, détruit ou sépare plusieurs éléments dont l'ensemble est vital, alors l'être vivant meurt.
Une forme vivante reste stable malgré les perturbations dues à l'environnement, elle doit être capable de s'adapter à des modifications de son milieu.
Les êtres vivants ont une capacité d'évolution au niveau des générations successives de l'espèce, cette propriété est nécessaire à la survie de l'espèce lors de changements importants de l'environnement. »

3. En outre, il y a presque autant de définitions que de personnes s'étant penchées sur le thème. Ainsi, John Stewart, étudiant le constructivisme et le cognitivisme[193], propose l'équation :

vie = cognition

Pour retrouver notre sujet, s'agissant des virus informatiques, il a cherché à voir s'il s'agissait d'une vie artificielle à travers une comparaison des propriétés minimales de tout système de vie

[192] http://www.math-info.univ-paris5.fr/~latc/va/va3.html
[193] Le cognitivisme est l'étude scientifique de la cognition; c'est-à-dire l'ensemble de processus mentaux tels la perception, la mémorisation, le raisonnement et la résolution de problèmes.

artificielle[194].

[194] http://www.vieartificelle.com

Définition générale	Cas particulier du virus informatique
L'être humain a contribué au processus d'apparition de tout système de vie artificielle ;	Oui
Un système de vie artificielle est autonome ;	Oui, il se reproduit et se propage seul
Un système de vie artificielle est en interaction avec son environnement ;	Oui, il analyse les fichiers, les sélectionne, les modifie
Il y a émergence de comportements dans un système de vie artificielle ;	Non, nous n'avons pas de nouveaux comportements qui apparaissent
Un système de vie artificielle peut se reproduire lui-même	Oui
Un système de vie artificielle possède une capacité d'adaptation ;	Oui, les virus fonctionnent avec des formats divers, avec des tailles de fichiers différentes, dans des environnements d'exploitation différents
Un système de vie artificielle n'est pas une unité. A l'opposé de la vie, un système de vie artificielle peut être réparti en plusieurs endroits : exemple, un robot et un ordinateur peuvent effectuer les calculs reliés par ondes. Même à l'intérieur d'un ordinateur, rien ne garantie que les octets de ce système sont tous regroupés.	Oui (qui plus est, un virus, peut se trouver en des systèmes d'information différents et distincts).

Ces quelques faits énumérés, il semble difficile de donner une réponse définitive à la question.

En effet, si nombre de comportements de la « vie » sont inhérents aux infections informatiques, Henri Bergson[195] estimait que « *Le rôle de la vie est d'insérer de l'indétermination dans la matière* » ; ce que le virus est, nous semble-t-il, encore incapable de réaliser (à oublier le principe même de la diffusion virale qui ne rentre pas dans le champ de cette citation).

[195] Henri Bergson (1859-1941), philosophe, auteur notamment de *Matière et mémoire* (1896), *Le rire* (1899), *L'évolution créatrice* (1907), *L'énergie spirituelle* (1919), *Les deux sources de la morale et de la religion* (1932) et Prix Nobel de littérature en 1928.

BIBLIOGRAPHIE

Entretiens

Corinne Moizan, ancienne attachée parlementaire de M. Jacques Godfrain lors de la rédaction de la loi du 5 janvier 1988.

Eric Filiol, chef de bataillon, chef du laboratoire de virologie et de cryptologie de l'Ecole Supérieure et d'Application des Transmissions.

François Paget, McAfee AVERT™, chercheur antivirus et « Chasseur de Virus » au sein de la société Network Associates, animateur du « Groupe Virus" au sein du CLUSIF.

Références bibliographiques informatives

[1] R. Anderson, « *Trusted Computing Fréquently Asked Questions TCPA/Palladium/NGSCB/TCG* », 2002 ;
disponible sur : http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html.

[2] Vesselin Bontchev, « *Are « good » computer viruses still a bad idea?* », 1995, disponible par ftp anonyme : ftp://ftp.informatik.uni-hamburg.de/ou 134.100.4.42.

[3] Léonard M. Adleman, *"An abstract Theory of Computer Viruses. In advances in Cryptology"*, CRYPTO'88, p. 354-374, Springer.

[4] Virus-L/comp.virus FAQ, disponible par FTP anonyme sur 138.23.166.133 ou sur http://www.faqs.org/faqs/computer-virus/faq/index.html

[5] Alan M. Türing, « *On Computable numbers with an application to the Entsheidung problem*", Proc. London Math. Society, 2, 42, p 230-265

[6] John von Neumann, "*Therory of Self-reproducing Automata*", 1966, édité et complete par Burcks, A.W., Univversity of Illinois Press, Urbana and London

[7] Eric Filiol, « *Les virus informatiques : théorie, pratique et applications* », Editions Springer, 2004, p.79 et suivantes.

[8] Ken Thompson, dans "*Reflections on Trusting Trust*", Communication of the ACM vol.27 n°8, August 1984. Réimprimé en 1995 et disponible sur http://www.acm.org/classics/sep95/

[9] Peter J. Denning ,"The Internet Worm" (1989)

[10] Rapport J. Thyraud Doc. Sénat 1987-88 n°3 p52

[11] Rapport J-J Hyest, Doc. Ass. Nat. 1991 N°2468, p. 113

[12] Mark A. Ludwig , « *Mutation d'un virus »,* ed. Adisson Wesley, 1994.

Ouvrages Techniques

Eric Filiol, « *Les virus informatiques : théorie, pratique et applications* », Editions Springer, 2004

Mark A. Ludwig, « *Naissance d'un virus* », Editions Addison-Wesley, 1993

Rod Daniels / Jack Clark, « *Virtual Technology : The first Examination of the parallels between cyberviruses and human viruses* », Network Associates.

Ouvrages Juridiques

Lamy, *Informatique et Réseaux*, sous la direction de M. Michel Vivant, 2004.

Alain Benssoussan, , Chapitre 1 « *Atteintes aux systèmes de traitement de données* », Mémento Françis Lefèvre, 1997p.791-806.

Alain Hollande, Xavier Linant de Bellefonds, « *Pratique du droit de l'informatique : Logiciels – Systèmes – Réseaux* », éd.Delmas, 5e éd., 2002.

Christiane Féral-Shuhl, « *Cyberdroit, le droit à l'épreuve de l'Internet* », éd. Dunod, 2002.

Trudel, Pierre, France Abran et al., « *Droit du Cyberespace* », Montréal, éd.Thémis, 1997.

Eric Caprioli, « *Consentement et systèmes informatiques* », Droit et Intelligence Artificielle, éd. Romillet, 2000.

Mémoires et Exposés

Mélanie Couhault, « *Les virus informatiques et l'avenir : Des ordinateurs aux téléphones portables* », DESS Droit du Multimédia et de l'Informatique, 2003.

Sébastien Calmont, « *Virus informatiques : De la protection à la responsabilité* », DESS Droit du Numérique et des Nouvelles Techniques, 2000.

Sophie Revol, « *Les logiciels espions* », DESS Droit du Multimédia et de l'Informatique, 2003.

Articles

01Net avec Reuters, « *Hoaxes : La peur du virus plus destructrice que le virus lui-même* », 14 mai 2001.

ADBS, Actualités du droit de l'information, « *Liste de diffusion* » N°29, octobre 2002, p. 3.

Antoine Gitton, « *I love you – Moi non plus* », Expertises, Juillet 2000, p. 214.

Bertrand Lemaire, « *Ersatz : Internet simulé dans des réseaux fermés* », Le Monde Informatique, 23 janvier 2004, n°1010, p.42.

Benoit Fechner : « François Paget : « *Les hackers sont loin de jouer avec un coup d'avance* » », L'Expansion, 25 juillet 2003.

Christophe Blaess, « Virus, nous sommes tous concernés ! », MISC n° 0 (http://www.miscmag.com/articles/index.php3?page=103).

Christophe Guillemin, « *Le FBI confirme l'existence de son logiciel espion* », ZDNet France, 14 décembre 2001.

Christophe Guillemin « *Les virus et leur dangerosité : les éditeurs pas toujours en accord* », ZdNet France, 18 octobre 2002.

Computer Economics, « *Economic Impact of Malicious Code Attacks* », 10 décembre 2001.

Daniel Guinier, « *Virus informatiques : Généricité contre polymorphisme, Mise en perspective des avancées en la matière* », Expertises, Mars 1998, p. 62.

Danielle Kaminski, étude pour le compte du CLUSIF : « Auteurs de virus, Entreprises, Editeurs d'antivirus : les liaisons dangereuses » (octobre 1998) ; commenté par Sylvie Rozenfeld, « *Responsabilité des éditeurs d'antivirus* », Expertises, novembre 1998, p. 328.

Emmanuel Jud, « *Jurisprudence Tati/Kitetoa : une faille dans la loi anti-piratage* », 14 avril 2003, Source Internet : Secuser.com

Edouard Launet, Laure Noualhat, « *Violente averse de virus* », Libération, 06 décembre 2001.

Eric Filiol, « *La lutte antivirale : techniques et enjeux* », MISC janvier-février 2003.

Etienne Wery, « *30 États signent la Convention sur la cybercriminalité* » ; Droit et nouvelles technologies, 23 novembre 2001.

Françoise Chamoux, « *La loi sur la fraude informatique : de nouvelles incriminations* », Semaine Juridique, éd. Gale I N°9 – 3321.

Frédéric Dechamps, « *Que faire en cas d?attaque contre son système informatique ?* », 21/08/02, Source : www.lex4u.com

Hervé Croze, « *L'apport du droit pénal à la théorie générale de l'informatique (à propos de la loi n°88-19 du 5 janvier 1988 relative à la fraude informatique)* », Semaine Juridique, éd. gale I N°18-3333

J. Devèze, « *Commentaire de la proposition de loi relative à la fraude informatique présentée par M. Jacques Godfrain le 5 août 1986* », Droit de l'Informatique, 1987, p. 44.

Jean Fiawoumo « *Les virus s'attaquent aux téléphones* », Le Monde.fr, 25 juin 2004.

Jean-Marc Manach, « *Quand un officier supérieur de l'armée tire à boulet rouge sur la LCEN* », ZDNET France, Jeudi 10 juin 2004.

JDNet Solutions, « *Virus : ce que l'avenir nous réserve* », 20 décembre 2002.

Ludovic Four, « *Sécurité informatique et besoins des utilisateurs : un compromis difficile* », Sécurité Informatique, n°49, juin 2004.

Marie Barel, *« Nouvel article 323-1 du Code Pénal : le cheval de Troie du législateur* », MISC n°14 (2004).

Michal Zaleski,, « "I don't think I really love you" or writing internet worms for fun and profit », 2000 ; (http://www.tla.ch/TLA/NEWS/2000sec/20000512Zalewski.htm).

Ministère de l'Économie, des Finances et de l'Industrie - Mission pour l'économie numérique le 23 janvier 2003 : http://www.men.minefi.gouv.fr/webmen/revuedeweb/virus.html

Murielle-Isabelle Cahen, « *Intrusion dans un système de traitement automatisé de données et aspiration d'un site Web : quels enjeux pour le droit ?* », 2 avril 2003, Source Internet : Serial Webbers.

Olivier Rafal, étude de Forrester Research « Is Linux More Secure than Windows ? » rapportée dans Le Monde Informatique, 16 avril 2004, N°1022, p.6.

Olivier Zilbertin « *Comment lutter contre les virus ?* », Le Monde Informatique, mercredi 10 mars 1999.

Pascal Lointier, « L'assurance contre les virus informatiques », MISC, n°5 (2003)

Débat avec Patrick Chambet, consultant en sécurité des systèmes d'information, « *Les virus informatiques menacent-ils Internet ?* » Le Monde.fr, 14 mai 2004.

Patrick Nicoleau, « *La protection des données sur les autoroutes de l'information* », Recueil Dalloz Sirey, 1996, Chro., 14e cahier, A.14.

Philippe Rocheteau, « *Droit des nouvelles technologies* », Présence-PC, 20 juillet 2004 (http://www.présence-pc.com/article-157.html).

Robert M. Slade, « *Viral Morality : A Call for Discussion* », 1995 (http://victoria.tc.ca/int-grps/books/techrev/virethic.txt).

Sylvie Rozenfeld, « *Responsabilité des éditeurs d'antivirus* », Expertises, novembre 1998, p. 328.

Thiébaut Devergranne, « *La loi « Godfrain » à l'épreuve du temps* », MISC n°2 (http://www.miscmag.com/articles/index.php3?page=304).

William B. Bierce, « *Le crime de violence technologique à New-York* », Expertises 1998.

Revues

Intelligence Artificielle.

MISC, Multi-system & Internet Security CookBook.

Sites Internet :

Virus Bulletin - Independent Anti-virus Advice : http://www.virusbtn.com/
Lettre d'information gouvernementale sur la société de l'information : http://www.internet.gouv.fr
Portail Sécurité.Org : http://www.securite.org
Un blog informatique : http://www.2607.info
Site de news informatiques : http://www.pcinpact.com/
Site du magazine MISC : http://www.miscmag.com/

Sélection de sites d'informations sur les virus : http://www.virusalerts.net; http://www.infovirus.org; http://www.secuser.com; http://www.zataz.com/reportages/virus.html; http://sun.soci.niu.edu/~rslade/mnvrrv.htm; http://www.infoplease.com/ipa/A0872842.html

Les sites de quelques éditeurs d'antivirus :

Trend Micro : http://fr.trendmicro-europe.com/

Mac Afee : http://fr.mcafee.com/
Symantec : http://www.symantec.fr/
Sophos : http://www.sophos.fr/
F-Secure : http://www.f-secure.fr/france
Kapersky: http://www.avp-france.com/

Jurisprudence

CA Douai 16 juin 1972, Gaz. Pal. 1972 2.722

CA Aix-en-Provence, 13 septembre 1972 ; JCP 1972 II. 17240, note A.C.

CJCE, 30 novembre 1976, aff. C-21/76, *Mines de potasse d'Alsace* : Rec. CJCE, p. 1735

Cass. Crim. « Logabax », 8 janvier 1979 ; Bull. Crim. N°13 ; Dalloz 1979. 509, note Corlay et IR. 182, obs. Roujou de Boubée ; Gaz. Pal. 1979.2.501 ; Rev. Sc. Crim. 1979.571, obs. Bouzat.

R. c. McLaughlin, 1980, 2 R.C.S.331, Comm Herbert et Pilon, Ottawa, SRBP, Ministère des Approvisionnements et Services Canada, 1992, pp. 11-13.

Cass. Crim. 9 mars 1987 ; Bull Crim. N°111 ; JCP 1988 II 20913, note Devèze ; Rev. Sc. Crim. 1988 311, obs. Bouzat
Cass. Crim. 12 janvier 1989, Bull. Crim. n°14.

Cass. Crim. « Antonioli », 1er mars 1989, Bull. Crim., 1989, n°100 ; Droit de l'informatique, 1990, p.38, note J.Huet.

TGI Paris, 5 janvier 1994 (http://www.textfiles.com/magazines/LNOIZ/lnoiz17.txt).

Cass. Crim. 5 janvier 1994 : Gaz. Pal. 1996 2 p. 419 note Catherine Latry-Bonnart.

CA Paris, 5 avril 1994 ; Dalloz 1994 IR 130.

Cass. Crim 30 mai 1996, Bull. Crim. 1996, n° 224, p. 625.

Cass. Crim., 12 décembre 1996, « Excelsior informatique », Comm J. Bertrand, Expertises, mars 1998, p. 70.

Cass. 1re civ., 14 janvier 1997, D. 1997, p.177

TGI Paris, 16 décembre 1997 ; Gaz. Pal. 1998 2. Somm. 433, note Rojinsky.

Cass. Crim. 14 novembre 2000, Bull. Crim. 2000, n°342, p. 1014.

TGI Le Mans 7 novembre 2003 (http://www.juriscom.net/jpt/visu.php?ID=390)