Revue de science criminelle 1998 p. 138

De diverses variétés de piratages..

Jacques Françillon, Professeur à la Faculté de droit Jean Monnet (Université Paris-XI)

Le terme « piratage », ou celui de « piraterie », recouvre, comme l'on sait, des réalités fort diverses : sur terre comme sur mer, dans l'espace comme... dans le « cyberespace ». Un commentateur de la *Gazette du Palais* (1er-2 août 1997, p. 10) faisait récemment état d'un article du journal *Ouest-France* (17 juin 1997) où il était question de pirates de la route qui rançonnent des automobilistes pour les délester de cartes bleues et de codes confidentiels, leurs mobiles étant évidemment d'une autre nature que ceux qui inspiraient Mandrin.

Pour aussi vague et peu juridique qu'il soit (Vivant et autres, *Lamy droit de l'informatique,* 1997, n° 2556 ; Gassin, *V°* Fraude informatique : *Rép. pén. Dalloz,* n° 2 et n° 162, 188 et 194), ce vocable n'en désigne pas moins, dans le domaine de l'immatériel, des formes de délinquance en pleine expansion, même si les procédures judiciaires concernant les contrefaçons de logiciels ou les accès frauduleux à des systèmes d'information demeurent encore marginales. Selon les statistiques de police judiciaire publiées par le ministère de l'Intérieur, 161 dossiers concernant la criminalité informatique auraient été traités en 1996 par des services de police et de gendarmerie, dont 25 ayant trait au piratage de logiciels, ce qui est peu (La Documentation française, 1997. - V. égal. *Expertises,* n° 207, août-sept. 1997, p. 253 : condamnation pénale des membres d'un réseau de distribution de logiciels piratés aux multiples ramifications internationales). Pour l'année 1994, les éditeurs de logiciels évaluaient pourtant à 57 % le nombre des copies contrefaisantes (D. Martin, *La criminalité informatique,* PUF, 1997, p. 27 et 28, citant les chiffres émanant de la Business Software Alliance). Certes, les estimations du Club de la Sécurité Informatique (Clusif) sont inférieures, et cet organisme note une baisse significative des attaques logiques et des contaminations virales. Il n'empêche que les pertes dues à la fraude informatique - toutes malveillances confondues - s'élèveraient à 2.3 milliards de francs en 1996 (*Expertises,* n° 203, mars 1997, p. 90). L'ampleur du phénomène, de même que l'importance des sinistres qui en résultent, traduisent la vulnérabilité d'une société de plus en plus dépendante de son environnement informatique (V. Guinier, « La guerre de l'information... », *Expertises* n° 208, oct. 1997, spéc. p. 307). Dans le « florilège des menaces » (*La criminalité informatique, ibid.*) qui pèsent sur elle, les piratages en tous genres ne sont cependant qu'une manifestation parmi d'autres d'une délinquance aux aspects multiformes, susceptible de compromettre la sécurité des systèmes d'information au sein des entreprises (V. le dossier « Sécurité et vices informatiques » publié par « Confidentiel-Sécurité »), aussi bien que de porter atteinte aux libertés individuelles et à la vie privée d'autrui (*17e rapport de la CNIL,* partie II, Les Enjeux : « Internet, liberté et vie privée ». - Rapprocher Crim. 4 mars 1997, *Bull. crim.* n° 83 : affaire dite des « écoutes de l'Elysée »). La licence des messages véhiculés par les réseaux - qu'il s'agisse du Minitel ou de l'Internet - est aujourd'hui trop préoccupante pour ne pas rendre indispensable l'intervention de mécanismes de régulation (V. not. en ce sens : *Internet, enjeux juridiques,* rapport Falque-Pierrotin, La Documentation française, 1996. - *Adde* : rapport de la Commission Beaussant, *Proposition de Charte de l'Internet,* 1997, spéc. la Présentation : pour une autorégulation de l'Internet). Parmi ces derniers, la procédure du référé remplit d'ores et déjà son office, tant au regard de la protection du droit d'auteur (TGI Paris, 14 août 1996, réf., deux espèces (*Brel et Sardou*), *D.* 1996.J.490, note Gautier ; *JCP* 1996.II.22727, obs. Olivier et Barbry ; T. com. Paris, 3 mars 1997, réf., *JCP* 1997.II.22840, obs. Olivier et Barbry. - *Adde* : Gautier, *D.* 1997, chron. 176. - Comparer, à propos de la diffusion non autorisée sur le réseau Internet de l'oeuvre de Raymond Queneau intitulée *Cent mille milliards de poèmes* : TGI Paris, 5 mai 1997, réf., *D.* 1997.IR.158, et *JCP* 1997.II.22906, obs. Olivier ; 10 juin 1997, réf., *Expertises* n° 207, sept. 1997, p. 271 et 283, et *JCP* 1997.II.22974, obs. Olivier et les références de la note 1 concernant d'autres ordonnances de référé) ou de la réputation d'autrui (V. en matière de diffamation TGI Paris,

30 avr. 1997, réf., *Gaz. Pal.* 19-21 oct. 1997.41, note Rojinsky ; *Expertises,* n° 208, oct. 1997, p. 320, note Givelet), qu'au regard de la lutte contre le racisme (TGI Paris, 12 juin 1996, et 10 juill. 1997, réf. (2 espèces : *Etudiants juifs de France*) : *Petites affiches,* 10 juill. 1996, p. 22, note Maisl ; *Expertises* n° 196, juill.-août 1996, p. 274 et 277, note Weber ; *Cahiers Lamy droit de l'informatique, Bulletin d'actualité* n° 94, juill. 1997, p. 6 et 7). Quant à la légitimité de l'intervention du droit pénal, elle demeure hors de doute eu égard à l'importance des valeurs à protéger (particulièrement lorsqu'il s'agit d'assurer la protection des mineurs contre la pornographie ou le proxénétisme) ; seules les modalités de cette intervention peuvent aujourd'hui encore prêter à discussion compte tenu des particularités de la communication en réseaux : responsabilité pénale des fournisseurs d'accès ou d'hébergement, loi applicable, etc. (Pour l'exposé des problématiques, V. parmi une littérature foisonnante : Chassaing, L'Internet et le droit pénal, *D.* 1996, chron. 329 ; Vivant, Cybermonde : Droit et droit des réseaux, *JCP* 1996.I.3969, spéc. II sur les aspects de droit pénal international. - *Adde* : *Internet saisi par le droit,* Travaux de l'AFDI, Editions des Parques, 1997 ; Proal, *La responsabilité du fournisseur d'information en réseau,* Presses Universitaires d'Aix-Marseille, 1997 ; Vergucht, *La répression des délits informatiques dans une perspective internationale,* Thèse Montpellier, 1996).

La délinquance liée aux technologies de l'information affecte également d'autres secteurs de la communication. Ainsi en est-il de la piraterie des oeuvres audiovisuelles (*new look* de la délinquance en col blanc, selon R. Schmelck, *in Mélanges Vitu,* Cujas 1989, p. 449 et s.). Qu'elle soit - comme la délinquance informatique - le fait de pirates amateurs ou de groupes mafieux organisés, elle se révèle très dommageable pour les titulaires de droits. Le commerce illicite le plus lucratif est évidemment celui des copies vidéo contrefaisantes. Celles-ci sont en effet réalisées à grande échelle dans des ateliers de reproduction clandestins, en France ou à l'étranger (V. le dossier spécial « Clef juridique de la vidéo multimédia et piraterie », *Gaz. Pal.* 11-12 oct. 1995, spéc. p. 7 : depuis la création de l'ALPA plus de 800 affaires de contrefaçon auraient ainsi été transmises aux parquets, 115 pour la seule année 1994. - *Adde* : *Le Monde* du 3 avr. 1997, article intitulé : « La Russie part en guerre contre le piratage des images »). Mais, dans le secteur télévisuel, il faut y ajouter une forme de piratage de plus en plus répandue : la réception sans paiement de services cryptés à péage. Il est clair qu'au moment où les techniques numériques du satellite et du câble permettent d'avoir accès à une infinité de programmes, proposés sous forme de bouquets, les intérêts commerciaux des exploitants de ces services seraient gravement compromis en l'absence d'interdiction de fabrication et de mise sur le marché de dispositifs de décodage non autorisés (V. notre étude *in Mélanges Vitu,* ouvrage préc., p. 211 et s. - *Adde* : Les captations non autorisées de programmes télévisés, *Actes du VIIIe Congrès de l'AFDP,* Economica 1986, p. 131 et s.). Les conclusions du *Livre vert* adopté par la Commission européenne le 6 mars 1996 - dont les réflexions ont principalement porté sur la recherche d'un niveau de protection juridique équivalent de manière à éviter des distorsions de concurrence entre les opérateurs des différents Etats membres - sont d'ailleurs en ce sens (doc. *COM* (96) 76 ; R.M. du 23 sept. 1996, *JOCE,* 19 déc. 1996 ; *Légipresse,* n° 130, II, p. 73).

Le rapprochement de certaines des techniques de piratage utilisées, ainsi que des décisions rendues en ces occasions par des juridictions pénales, n'est pas sans intérêt (on exclura du champ de cette étude les décisions portant sur des actes de contrefaçon).

PIRATAGES INFORMATIQUES

Fraudes télématiques

Connexions frauduleuses à des serveurs de jeux

L'arrêt rendu par la cour d'appel d'Aix-en-Provence le 23 octobre 1996 (publié tardivement par la *Gazette du Palais* des 20-22 juill. 1997, p. 34, avec une note signée Latry-Bonnard) est intéressant à un double titre. D'une part, il confirme l'application en matière de télématique des incriminations issues de la loi Godfrain du 5 janvier 1988 (c. pén., art. 462-2 et s. anc. ; art. 323-1 et s. nouveaux). D'autre part, il marque la spécificité de ces incriminations par rapport aux qualifications traditionnelles de vol et d'escroquerie.

Plusieurs techniciens de France Télécom avaient, à l'insu de leur hiérarchie, raccordé

clandestinement un terminal Minitel à une ligne d'essai et l'avaient branché sur un serveur de jeu télématique. A chaque prise de service, ils l'activaient et le connectaient sur le réseau 3615 Playtel, lequel proposait des lots à gagner sous forme de bons d'achat capitalisés en fonction du temps d'utilisation, bons d'achat que les techniciens percevaient après avoir communiqué au serveur, chaque semaine, et à tour de rôle, leurs coordonnées personnelles. Le Minitel - auquel avaient été ajoutés par la suite trois autres terminaux dissimulés sous un faux plancher - fonctionnait en continu toute la journée, les traces de cette utilisation abusive étant effacées grâce à une manipulation technique. Il en était évidemment résulté un important préjudice pour France Télécom en raison des taxes téléphoniques dues, dont les deux tiers devaient être reversés au serveur (préjudice évalué à 750 000 F environ).

Les poursuites pénales engagées contre les prévenus l'avaient été initialement pour vol. Mais cette qualification ne pouvait être retenue, la Chambre criminelle considérant les communications téléphoniques comme des prestations de service non susceptibles d'appropriation (Crim. 12 déc. 1990 (*Tondoux*), *Bull. crim.,* n° 430 ; *D.* 1991.J.364 , note Mirabail, où il s'agissait également d'une hypothèse d'utilisation abusive d'un terminal Minitel). Au même titre que les données informatiques, ou toute autre information envisagée indépendamment de son support, de telles prestations n'entrent pas en effet dans la catégorie des choses susceptibles de vol (pour le rejet de cette dernière qualification en cas de transferts de logiciels : Paris, 25 nov. 1992, *Gaz. Pal.* 1994.3.474, note Latry-Bonnard, et *Gazette du droit des technologies avancées,* n° spécial, oct. 1996, p. 286, *Gaz. Pal.* 1994.3.474, note Latry-Bonnard ; et en matière de recel : Crim. 3 avr. 1995, *Bull. crim.,* n° 142 ; cette *Revue* 1995.599 , et nos obs.). Certes, depuis l'entrée en vigueur du nouveau code pénal, les possibilités de répression sont accrues du fait de l'extension de l'escroquerie aux cas où la dupe se borne « à fournir un service ». Mais, s'agissant comme en l'espèce de faits antérieurs au 1er mars 1994, cette dernière qualification n'avait pas été envisagée (V. cependant parmi les arrêts retenant l'escroquerie : Crim. 4 mai 1987, *Bull. crim.,* n° 175, pour un trucage de communications téléphoniques reçues de l'extérieur ; 13 déc. 1990, *ibid.,* n° 435, pour une connexion permettant aux gérants d'un centre serveur d'obtenir la rétrocession de redevances télétel indues).

Quoi qu'il en soit, faute pour les prévenus d'avoir été autorisés à utiliser comme ils l'avaient fait les lignes d'essais et les terminaux de France Télécom, les délits d'accès et de maintien frauduleux dans un système de traitement automatisé de données étaient caractérisés dans leurs éléments tant matériel que moral (en ce sens note Latry-Bonnard, préc.). Une connexion par Minitel ne saurait en effet être régulière à défaut d'habilitation par la loi, le contrat ou la volonté du maître du système : il en est ainsi dès lors que les procédés utilisés établissent que l'agent a su qu'il agissait sans droit (Gassin, *Rép. pén. Dalloz,* n° 132). Inversement, il a été jugé que les connexions effectuées en vue de télécharger gratuitement, toutes les 2 minutes 59 secondes, et grâce à 25 micro-ordinateurs branchés sur 25 lignes téléphoniques, les annuaires de France Télécom, ne tombaient pas sous le coup de telles incriminations (Rennes, 6 févr. 1996, *Expertises* n° 199, nov. 1996, p. 406, obs. Bertrand ; *Cahiers Lamy droit de l'informatique, Bulletin d'actualité,* n° 86, nov. 1996, p. 7 et 8). Il est vrai que la question avait été posée en doctrine de savoir si ces dernières protègent l'abonné, à l'insu et contre le gré duquel le Minitel a été utilisé, au même titre que le maître du système, c'est-à-dire « la personne ou le service compétent pour autoriser l'accès » (Devèze, *J.-Cl. Pénal,* art. 323-1 à 323-7, n° 31 *in fine*), alors même que ce dernier ne subirait pas un véritable « préjudice informatique » (V. note Mirabail préc., II, texte et note 32). A cette question, l'arrêt ici commenté, ainsi que d'autres décisions (V. *infra,* I, 3°), apportent une réponse positive : l'essentiel aux yeux des tribunaux, pour caractériser les délits de l'article 323-1, alinéa 1, du code pénal, est d'établir que les prévenus ont eu conscience d'usurper le droit à l'accès ou au maintien dans un système.

Neutralisation frauduleuse du dispositif de déconnexion automatique par la technique dite du « rafraîchissement d'écran »

Un jugement du tribunal correctionnel de Paris du 5 novembre 1996 (*Expertises,* n° 202, févr. 1997, p. 81, obs. Bertrand ; *Cahiers Lamy droit de l'informatique, Bulletin d'actualité,* n° 89, févr. 1997, p. 9 et 10) fournit des précisions concernant l'une des techniques utilisées par les

fraudeurs : le « rafraîchissement d'écran ». Il s'agit d'un procédé permettant de faire obstacle à la procédure de déconnexion automatique mise en place par France Télécom après chaque séquence de 5 minutes sans transfert de données. L'intérêt d'une telle procédure pour le consommateur distrait est évident puisqu'à partir du « décrochage » il n'a plus rien à payer. Mais l'intérêt de la technique consistant à paralyser ladite procédure était, ainsi qu'on va le voir, tout aussi évident pour les prévenus.

Il s'agissait, pour la plupart d'entre eux, d'agents de France Télécom chargés de la maintenance des installations téléphoniques du palais de justice de Paris, du Sénat et de divers ministères. Comme dans l'affaire précédente, ils avaient participé intensivement à des jeux télématiques, ici encore sans bourse délier et à des fins moins ludiques que lucratives, leur but étant de multiplier le nombre de points leur ouvrant droit à des cadeaux. Or leur fraude reposait sur le fait - naturellement connu d'eux - qu'un compteur de points (automatiquement mis en oeuvre toutes les 35 secondes) avait été inclus dans le logiciel de jeu des deux centres serveurs auxquels ils s'étaient connectés, compteur destiné à « rafraîchir » en permanence l'écran et donc à neutraliser le temporisateur de surveillance de trafic de France Télécom.

A l'égard des joueurs, le tribunal retient non le délit d'accès, mais celui de maintien frauduleux dans un STAD. Admettant la régularité de la connexion initiale en l'absence de « procédé malin ou frauduleux », il considère, en revanche, que le temps écoulé jusqu'au débranchement, loin de constituer une abstention non punissable comme il était soutenu, « contient en lui-même l'action de faire durer la connexion », ce dont les intéressés ont été « les seuls arbitres ». A l'égard du gérant de l'un des centres serveurs, concepteur et exploitant du logiciel litigieux, le tribunal retient le délit d'entrave au fonctionnement d'un STAD. Cette qualification s'imposait d'autant plus en l'espèce que le prévenu était parfaitement informé de l'existence et des implications du système de surveillance établi par France Télécom, ne serait-ce qu'en raison de la convention Kiosque souscrite par lui. L'un des intérêts de la décision commentée réside précisément dans le fait qu'elle admet la responsabilité pénale des centres serveurs télématiques, dès lors du moins que ceux-ci ont été partie prenante à la fraude (V. en ce sens note Bertrand, préc., qui fait le rapprochement avec la responsabilité des serveurs de messageries). Mais cette décision met également en évidence les limites de la répression des délits informatiques dans la mesure où les délits d'escroquerie et de recel ont également été retenus en l'espèce (respectivement à la charge du gérant et des joueurs). On peut donc craindre que les incriminations spécifiques issues de la loi Godfrain n'aient en définitive qu'une utilité réduite.

Racolage automatisé de clientèle

Les tribunaux ont eu à plusieurs reprises l'occasion d'appliquer les dispositions pénales réprimant les fraudes informatiques aux procédés, aujourd'hui bien connus, qui tendent à fausser la concurrence entre les services télématiques, et l'on sait que cette concurrence est particulièrement vive quand elle oppose des « messageries roses ». Les agissements répréhensibles consistent à injecter dans le réseau téléphonique un grand nombre de messages - « vides », non désirés ou de « contre-information » destinés à inciter les « minitelistes » à se connecter sur des services concurrents de ceux auxquels ils s'adressent habituellement. Cette injection se fait à l'aide de micro-ordinateurs et grâce à des programmes d'appels partiellement ou totalement automatisés, simulant la connexion de plusieurs Minitels, et ce dans des conditions permettant d'échapper aux contrôles (connexions brèves, suivies de reconnexions immédiates sous un pseudonyme différent). C'est peu dire que les techniques de racolage systématique utilisées ont fait la preuve de leur efficacité : il a par exemple été établi, à la suite d'une des enquêtes diligentées par la police judiciaire sur commission rogatoire, que, pour un message de 33 caractères, l'utilisation d'un micro-ordinateur programmé à cet effet avait permis d'adresser ledit message à une centaine de personnes en moins d'une minute. Les conséquences préjudiciables de telles pratiques sont évidemment fort préoccupantes pour les fournisseurs de services télématiques concurrents dont les boîtes aux lettres, de même que les lignes Transpac, sont très vite saturées ; en outre, les performances de leurs systèmes sont considérablement réduites du fait des ralentissements de la capacité des centres serveurs concernés, voire de leur arrêt momentané

dû à l'impossibilité de supporter la surcharge d'appels. Quant aux parades techniques existantes - des dispositifs de surveillance « anti-piratage » pourtant sophistiqués - , elles se sont souvent révélées insuffisantes en raison du nombre, de la fréquence ou de la simultanéité de ces connexions parasites. Il n'y a donc guère que la voie des poursuites pénales qui soit de nature à faire échec à ce type d'agressions par automates d'appel.

C'est cette voie qui a été choisie - avec les avantages qu'elle procure du point de vue de la recherche des preuves - dans plusieurs affaires. La plus récente a donné lieu à un arrêt de la cour d'appel de Paris du 14 janvier 1997 (*Cahiers Lamy droit de l'informatique, Bulletin d'actualité,* n° 97, nov. 1997, p. 12) qui reprend l'essentiel de la motivation d'un précédent arrêt remarqué de la même cour (Paris, 5 avr. 1994, *D.* 1994.IR.130 ; *JCP* 1995, éd. E, I, 461, obs. Vivant et Le Stanc ; *Petites affiches* 1995, n° 80, p. 13, note Alvarez ; *Dr. informatique et télécoms* 1996/3, p. 51, note Alvarez. - *Adde* : Gassin, *Rép. pén. Dalloz,* n° 89, 103, 132, 169... ; Devèze, *J.-Cl. Pénal,* art. 323-1 à 323-7, n° 21, 31, 34, 39, 45...). Il n'y a donc pas lieu de s'étendre sur le sujet, sinon pour observer que, dans les deux cas, la plupart des prévenus (parmi lesquels figurent naturellement les concepteurs et exploitants des logiciels de « racolage ») ont été condamnés, d'une part pour *maintien* frauduleux dans un STAD (et non accès, car la connexion par le 36.15 ouvert au public était régulière) (art. 323-1, nouv.), d'autre part pour *entrave* à son fonctionnement (art. 323-2, nouv.), et ce sur la base de principes désormais bien établis : non-exigence d'un dispositif de sécurité protégeant contre les intrusions ou les autres atteintes ; maintien frauduleux fondé sur les idées d'interversion de titre, de défaut d'habilitation et de non-respect de la « règle du jeu » - opposable à tous les utilisateurs du service - fixée par la loi, le contrat ou le « maître du système » (celui qui, selon la cour, a « compétence pour disposer du système ou décider de sa conception, de son organisation ou de ses finalités ») ; existence d'actes positifs d'entrave, révélant par eux-mêmes l'intention de fraude, et ayant indifféremment pour effet soit de bloquer le système attaqué, soit seulement d'en perturber le fonctionnement. A cela s'ajoute encore le fait qu'au titre de l'accès frauduleux - et non par simple inadvertance - sont visés tous les modes de pénétration irréguliers, y compris à distance ou en cas de travail sur la même machine mais à un autre système... On voit que cette jurisprudence assure un niveau élevé de protection aux éditeurs informatiques dont les serveurs font l'objet d'instrusions abusives en vue de « capter » leur clientèle.

Autres manipulations frauduleuses
Introduction frauduleuse de données
Selon les études statistiques émanant des assureurs, une grande partie des malveillances informatiques recensées (80 %) proviendraient de l'intérieur des entreprises (Martin, *La criminalité informatique,* ouvrage préc., p. 13). Une décision du tribunal correctionnel de Thionville du 3 juin 1997 en fournit une illustration (*Expertises,* n° 208, oct. 1997, p. 317, obs. Bertrand).

Dans cette affaire, un salarié de la Caisse régionale d'assurance maladie d'Ile-de-France avait conçu un programme de piratage et l'avait introduit dans le système informatique de la Caisse, système qu'il avait préalablement détérioré de manière à être appelé à se rendre sur place pour en assurer la maintenance. Ce programme était destiné à identifier les transferts de fonds importants vers certains fournisseurs et à détourner ces fonds par l'intermédiaire de deux sociétés dont des acolytes avaient pris le contrôle pour récupérer l'argent. L'opération de piratage proprement dite s'inscrivait donc dans le cadre d'une fraude de grande envergure ayant permis de détourner une somme de plus de 17 millions de francs. Tous les prévenus avaient été poursuivis pour escroquerie en bande organisée et condamnés à des peines sévères, dont quatre ans d'emprisonnement pour l'instigateur de la fraude, cinq ans pour le coordonnateur du groupe et trois ans pour le salarié ayant implanté le programme-pirate. Les manoeuvres frauduleuses étaient en effet constituées par la falsification des bandes de paiement informatiques, et l'escroquerie n'avait pu être réalisée qu'en raison de la compétence technique et de l'intervention directe de ce dernier prévenu, ce que précise le tribunal. C'est du reste la raison pour laquelle le jugement ne comporte aucune analyse des éléments constitutifs des délits spécifiquement informatiques, qui fondaient également la prévention.

Mais il est clair que ces délits étaient caractérisés en l'espèce, qu'il s'agisse de l'accès frauduleux à un STAD (art. 323-1, al. 1) ou de l'introduction, de la suppression ou de la modification frauduleuse de données (art. 323-3) : le premier, en raison du subterfuge utilisé par le programmateur pour pouvoir accéder aux bandes correspondant à la chaîne de paiement des fournisseurs ; le second, du fait de la falsification de ces bandes. Certes, à la différence de l'ancien article 462-5 issu de la loi du 5 janvier 1988, le code pénal n'incrimine plus le « faux informatique » en tant que tel. Mais le délit d'atteinte volontaire aux données contenues dans un STAD demeure, quant à lui, constitué dès l'instant où ce sont les données elles-mêmes qui se trouvent manipulées ou altérées sans droit au sein d'un tel système, ce qui était bien le cas ici.

C'est d'ailleurs cette dernière qualification qui avait été retenue dans l'affaire ayant donné lieu à l'arrêt de la Chambre criminelle du 5 janvier 1994 (*JCP,* éd. E, 1994.I.359, obs. Vivant et Le Stanc ; *Cahiers Lamy droit de l'informatique, Bulletin d'actualité,* n° 81, mai 1996, p. 1 et s., commentaire Gassin). La malveillance commise par une salariée responsable du service informatique, peu avant son départ de la société qui l'employait, avait d'abord consisté à porter sur des fiches manuscrites de saisie informatique des renseignements inexacts concernant le code du taux de TVA applicable aux produits de la société, puis à les introduire en partie elle-même dans le système de gestion informatisé de l'entreprise en vue de constituer un fichier-produits, situation qui avait eu pour effet de retarder la mise en place définitive de ce système, lequel était en cours d'élaboration à l'époque. Cet arrêt a été d'autant plus remarqué en doctrine (V. particulièrement le commentaire approfondi de M. Gassin) qu'il retient une conception relativement large de l'élément matériel - caractérisé même en cas d'introduction matérielle de données par un tiers - , et fort simplifiée de l'élément moral - « nécessairement » caractérisé par l'introduction volontaire de données inexactes.

Il est vrai que, dans l'affaire ayant donné lieu au jugement commenté, il n'eût été nullement nécessaire d'admettre des solutions extensives pour justifier la condamnation du programmateur-pirate sur le fondement de ce texte d'incrimination.

Virus informatique

La fameuse affaire du virus *FRODO* n'a pas encore trouvé son épilogue judiciaire. Elle avait pourtant débuté le 10 avril 1991 par la contamination de disquettes publicitaires comportant un aperçu du logiciel de bureautique *Vega* que la revue *Soft et micro* - disparue depuis lors ! - avait vendues avec l'un de ses numéros. « Cadeau » empoisonné, donc, pour les nombreuses victimes. Celles-ci doivent être à l'heure actuelle d'autant plus dépitées des pannes successives du dossier qu'il leur était permis d'espérer qu'après trois ans d'instruction et deux rapports d'expertise la justice serait suffisamment éclairée pour répondre à la question de savoir qui était à l'origine de la diffusion du virus : était-ce la société qui avait conçu et commercialisé le logiciel *Vega,* celle qui avait réalisé la disquette maîtresse, ou celle qui l'avait dupliquée en 65 000 exemplaires ? Or, à la mi-septembre 1997, la 11e Chambre de la cour d'appel de Paris en était encore à écouter l'avocat général et les conseils des parties avant de juger de l'opportunité de désigner un nouvel expert (*Expertises* n° 208, oct. 1997, p. 290). Il est vrai qu'entre-temps une lourde condamnation pénale était intervenue à l'encontre de deux informaticiens, que celle-ci avait été infirmée en appel, les prévenus ayant été relaxés au bénéfice du doute (Paris, 15 mars 1995, *JCP* 1995, IV, n° 1425, p. 182 ; *Expertises,* 1994, p. 441 ; *Cahiers Lamy droit de l'informatique, Bulletin d'actualité,* n° 72, juill.-août 1995, p. 8 et 9), et que l'arrêt de la cour avait été censuré au motif, notamment, que des auditions et d'autres mesures d'investigation auraient dû être ordonnées en raison des lacunes de l'information relevées par les seconds juges (Crim. 12 déc. 1996, *Bull. crim.* n° 465 ; *Expertises,* n° 203, mars 1997, p. 114, obs. Beaujard). Le moins que l'on puisse dire est que la situation est devenue embarrassante pour tout le monde : à la légitime inquiétude que suscitent les infections de logiciels et de réseaux dans une société de plus en plus informatisée (Bismuth, Virus, la grande peur du XXe siècle, *Expertises,* 1989, n° 141. - *Adde* : Burger, *Virus, la maladie des ordinateurs,* éd. Micro application, 1989), s'ajoute désormais la crainte que la justice pénale ne soit impuissante face à ce type d'agressions informatiques.

Quoi qu'il en soit de ces péripéties et de ces atermoiements, l'arrêt de la Chambre criminelle ne manque pas d'intérêt. Car, sur le plan pénal, et en dehors des aspects purement probatoires, ce sont les éléments constitutifs des délits d'atteinte au fonctionnement des systèmes (art. 462-3, anc., et 323-2 nouv.) et d'atteinte aux données contenues dans ces systèmes (art. 462-4, anc., et 323-3 nouv.) qui se trouvent précisés.

Il n'était pas seulement reproché aux prévenus d'avoir introduit délibérément un virus dans le logiciel lors du compactage des données. Il leur était fait grief, en outre, de ne pas avoir informé le client de la présence de ce virus sur les disquettes, préalablement à la distribution de celles-ci. La principale victime, la société éditrice de la revue *Soft et micro,* prétendait que les prévenus avaient eu, à tout le moins, connaissance de l'infection du master au cours des opérations de duplication. Elle se fondait sur la constatation, par les experts, d'une tentative de suppression du virus (en rapport, semble-t-il, avec la confection d'un nouveau master). La cour de Paris n'ayant pas répondu à des conclusions qui, selon la Chambre criminelle, « faisaient valoir que l'intention frauduleuse des prévenus se déduisait de leur parfaite connaissance du diagnostic et des traitements anti-virus », son arrêt est donc également censuré pour ce motif. Le sommaire au *Bulletin* (p. 1354) en tire la conclusion - de manière plus explicite que ne le fait apparaître le texte même de l'arrêt (V. sur cette pratique les réserves de Ph. Conte, note au *D.* 1997.J.615 , spéc. note 5, *in fine*) - que les délits objet des poursuites sont constitués par « le fait de s'abstenir d'informer (un client) de l'introduction, même accidentelle, d'un (tel) virus, lorsqu'on en a connaissance, ainsi que de l'altération de l'ensemble du système informatique qui peut en résulter lors de la mise en oeuvre du logiciel (infecté) ».

C'est dire - si, du moins le résumé ne travestit pas la substance de l'arrêt (*ibid.*) - que les incriminations susceptibles de s'appliquer aux malveillances de cette nature seraient désormais envisagées par la jurisprudence d'une manière singulièrement extensive. Qu'une telle extension soit justifiée par le souci d'assurer un haut niveau de sécurité informatique, y compris sur le plan juridique, ceci est fort louable et peut contribuer à dissiper le malaise résultant de l'ineffectivité actuelle du dispositif pénal dans l'affaire *FRODO,* ainsi que nous l'avons noté précédemment. Il n'en demeure pas moins que l'assimilation ainsi réalisée d'un défaut d'information à un acte positif d'entrave ou d'altération n'est guère en accord avec les principes du droit pénal, sauf à considérer que la loi incrimine une sorte de mise en danger délibérée des systèmes informatiques au même titre que l'atteinte volontaire - consommée ou seulement tentée - à ces systèmes ou aux données qu'ils contiennent. On se ralliera par conséquent à la seule doctrine respectueuse du principe de légalité, celle qui définit l'entrave au sens de l'article 323-2 du code pénal comme le fait d'empêcher un système de fonctionner « par une action positive » (Gassin, *Rép. pén. Dalloz,* n° 169 ; Devèze, *J.-Cl. Pénal,* n° 55), que cette action conduise à bloquer ou seulement à perturber ce fonctionnement, situation qui correspond bien aux hypothèses d'introduction de « virus » ou autres « bombes logiques » (*Adde* : Bloch, Virus : responsabilité pénale, *Expertises,* 1989, n° 114 ; Gautier, Les virus informatiques et le droit pénal, *Travaux de l'Institut de droit des affaires d'Aix-Marseille,* 1990). Quant au texte de l'article 323-3, qui vise les actes portant atteinte à l'intégrité du contenu du système, il parle de lui-même : son énumération n'inclut que les « modes d'action » sur les données (Gassin, *op. cit.,* n° 199). Admettre une conception trop extensive des éléments tant matériels que moraux de ces délits conduirait à assimiler à des malveillances caractérisées (Paris, 5 oct. 1994, *JCP* 1995, éd. E, I, 461, obs. Vivant et Le Stanc : modification de données portant sur le programme des clefs d'accès et aboutissant à bloquer le système) des comportements moralement et socialement irréprochables (V. pour une hypothèse de relaxe du chef d'entrave, parfaitement justifiée, trib. corr. Poitiers, 26 juin 1997, *Gaz. Pal.* 29-30 oct. 1997, p. 21 ; *Expertises,* n° 207, août-sept. 1997, p. 248 : ingénieur brutalement mis à pied sans avoir pu expliquer le mode de fonctionnement du système de verrouillage informatique mis en place par lui).

PIRATAGES AUDIOVISUELS

L'arrêt de la Chambre criminelle du 14 mai 1997 (*Bull. crim.* n° 184) est relatif aux délits prévus par les articles 79-1 à 79-4 de la loi du 30 septembre 1986 (anciens art. 429-1 à

429-4 du code pénal). Il fait suite à deux précédents arrêts de la même Chambre (Crim. 23 mars 1992, *Bull. crim.* n° 124 ; 19 août 1992, *ibid.,* n° 277) qui avaient fourni d'intéressantes précisions sur les éléments constitutifs de ces infractions (*Dr. pénal* 1993, comm. 82, note Véron ; cette *Revue* 1993.563 et 565, et nos obs.). Le premier concernait des actes se situant en amont de la captation proprement dite des programmes télédiffusés à péage (fabrication et commercialisation de décodeurs pirates) ; le second visait des opérations situées en aval de cette captation (réinjection par un syndic de copropriété, sur le réseau de télédistribution d'un ensemble immobilier, de programmes préalablement et régulièrement décryptés grâce à un décodeur loué à la société Canal Plus) ; les pourvois formés contre les arrêts de condamnation avaient été rejetés dans les deux cas. Il ressortait de ces décisions : d'une part, qu'en incriminant les captations frauduleuses de tels programmes la loi « réprime nécessairement le décryptage de ces programmes en violation des droits de l'exploitant » ; d'autre part, qu'en incriminant de manière distincte l'organisation frauduleuse de leur réception par des tiers, la loi « réprime nécessairement la mise en oeuvre de tout procédé procurant à autrui... l'accès (indu) à ces programmes... ».

A première vue, le champ de la répression paraît s'être encore élargi avec la décision ici commentée, en ce qui concerne du moins le délit de détention en vue de la vente et de vente de décodeurs pirates. En revanche, s'agissant des autres qualifications retenues par l'arrêt attaqué - organisation frauduleuse de la réception et achat de décodeurs pirates en vue de leur utilisation - , la Chambre criminelle ne se prononce pas sur le fond, les seconds juges ayant outrepassé les limites de leur saisine ; elle se borne donc à faire application de la peine justifiée. Les faits de l'espèce méritent cependant d'être analysés sous leurs différents aspects.

Commercialisation de matériels de décodage pirate

Des composants électroniques nécessaires à la fabrication de décodeurs pirates avaient été acquis en pièces détachées par un employé de France Télécom. Ces composants, conditionnés en kit, étaient conçus pour entrer dans le montage de décodeurs. Ils avaient été commercialisés en l'état, et en grande quantité, notamment auprès de collègues de travail, dont certains les avaient revendus après les avoir assemblés à l'aide de la notice de montage qui leur avait été remise. Il ne s'agissait donc pas d'un acte de piratage isolé et ludique, mais d'une fraude d'envergure. On était loin du cas de cet électronicien astucieux qui avait été condamné pour avoir fabriqué un appareil muni d'un logiciel lui permettant de décrypter des émissions sans avoir besoin du code transmis mensuellement par Canal Plus à ses abonnés (Trib. corr. Angers, 6 mai 1988 (inédit), cette *Revue* 1989.516, obs. Bouzat). L'intéressé avait pourtant déclaré à l'époque au tribunal qu'il aimait le bricolage, qu'il était passionné, et que s'il avait créé cet appareil ce n'était pas pour frauder mais par goût de la recherche ; propos qui n'avaient que partiellement réussi à attendrir les juges puisque ces derniers avaient retenu la qualification la moins sévère de toute la panoplie légale : celle de détention de matériel pirate en vue de son utilisation (art. 429-4, ancien, c. pén. ; aujourd'hui art. 79-4 L 30 sept. 1986). Cela étant, lorsque le piratage revêt une toute autre ampleur, il est compréhensible qu'une qualification plus grave soit retenue. Tel avait été le cas en l'espèce, le prévenu ayant été condamné à 9 mois d'emprisonnement avec sursis et 40 000 F d'amende, ainsi qu'au versement d'une somme de 180 000 F à titre de réparation pour le préjudice subi par l'exploitant (Canal Plus également en l'occurrence).

Sur le plan pénal, le demandeur au pourvoi prétendait que les faits qui lui étaient reprochés ne pouvaient tomber sous le coup de l'incrimination de l'article 429-1 du code pénal (L 1986, art. 79-1, nouveau, dont les termes demeurent inchangés). Il faisait en effet valoir que si les composants litigieux étaient bien « conçus en vue du captage », ils n'étaient pas « en eux-mêmes aptes au captage ». Mais la Chambre criminelle écarte sèchement l'argument : « il n'importe... que le matériel conçu pour capter frauduleusement des programmes télévisés, vendu en pièces détachées, suppose un montage pour son utilisation ».

Certes, la circonstance que des schémas de montage avaient été fournis en même temps que ces composants n'a probablement pas été indifférente pour justifier le rejet du pourvoi. Mais c'est moins pour une raison de fond que pour une raison de preuve. En effet, cette

circonstance établissait non seulement que les pièces litigieuses avaient été *conçues* pour entrer dans le montage de décodeurs compte tenu de leur mode de conditionnement - ce que le prévenu ne contestait pas - , mais qu'elles étaient *aptes,* en outre, à remplir leur fonction dans l'opération de décodage une fois effectué l'assemblage de tous les éléments du kit ; la matérialité du délit était dès lors caractérisée. Elle démontrait également la volonté du prévenu de contribuer à rendre ce matériel opérationnel grâce aux instructions fournies, sachant que des tiers allaient pouvoir accéder ainsi, sans droit, à des programmes télévisés à péage ; l'intention frauduleuse était par suite établie. A défaut de telles instructions, cette double preuve aurait pu résulter d'autres circonstances, ou tout simplement de l'aveu du prévenu qu'il avait acheté et revendu dans ce dessein des matériels présentant les caractéristiques recherchées.

Quant au fond, l'extension de l'incrimination est plus apparente que réelle par rapport aux décisions antérieures. Car la loi vise tout « équipement, matériel, dispositif ou instrument conçu en tout ou partie » dans une finalité de fraude, énumération qui englobe par conséquent tout composant, électronique ou autre, ayant pour particularité d'avoir été spécifiquement conçu à cette fin, quel que soit son mode de conditionnement ou de fonctionnement. La solution de l'arrêt s'inscrit ainsi parfaitement dans le cadre d'un dispositif légal qui tend à éviter le passage à l'acte de piratage proprement dit et à protéger le mieux possible les droits des exploitants (V. nos obs. préc., spéc. p. 565). On se souvient d'ailleurs que c'est en raison de l'inadaptation des qualifications de droit commun qu'une cour d'appel avait prononcé la relaxe dans l'affaire de la publication des plans du décodeur de Canal Plus (Paris, 24 juin 1987, *Gaz. Pal.* 1987.2.512, obs. Marchi ; *DS* 1988, Somm. 226, obs. Hassler ; Bouzat, cette *Revue* 1988.793. - *Adde* : *Lamy droit de l'informatique,* 1997, n° 2554) et que c'est pour remédier à ce qui lui était apparu comme une lacune de la répression que le législateur était intervenu pour mettre fin à ce type d'incitations (L 10 juill. 1987 : c. pén., art. 429-2, anc. ; L 1986, art. 79-2, nouv.). Certes, dans le passé, des réserves avaient été émises en doctrine sur l'opportunité d'une telle législation au regard des libertés publiques (obs. Bouzat, préc.). Mais elles sont aujourd'hui totalement dépassées en raison de l'explosion des nouvelles technologies et de l'importance des intérêts économiques en jeu (V. *supra*).

Sur le plan civil, la société Canal Plus invoquait d'abord un préjudice matériel résultant de la diffusion des décodeurs pirates : perte d'abonnés potentiels et privation de contrepartie financière, ses investissements en matière de programmation n'ayant pas été rentabilisés comme ils auraient dû l'être. Elle estimait ensuite avoir souffert d'un préjudice moral, celui-ci étant constitué par l'atteinte portée à l'image de la société Canal Plus, tant aux yeux des abonnés réguliers qu'à ceux des auteurs et compositeurs titulaires des droits de diffusion. Même si l'on peut ne pas être totalement convaincu quant à la réalité de ce dernier préjudice, force est de reconnaître que les dommages-intérêts alloués par les juges du fond, dont les énonciations sont reprises et approuvées par la haute juridiction, ont un évident caractère punitif et... dissuasif.

Organisation frauduleuse de la réception pirate

Même si la Chambre criminelle n'a pas eu à se prononcer sur le fond (*supra*) s'agissant du délit d'organisation frauduleuse de la réception par des tiers de programmes télédiffusés réservés à un public déterminé (art. 429-3, anc., c. pén. ; art. 79-3, nouv., L 1986), il n'est pas sans intérêt d'observer que la cour d'appel a considéré pour sa part que ce délit était caractérisé en l'espèce par le simple fait pour le prévenu d'avoir fourni à certaines personnes les codes nécessaires pour capter en clair les émissions cryptées de Canal Plus. Certes, en prévoyant cette incrimination spéciale, le législateur avait principalement en vue les procédés techniques divers permettant à des tiers de recevoir gratuitement des programmes qui ne leur sont pas destinés (V. notre étude au *J.-Cl. Pénal,* art. 429-1 à 429-5, anciens), Protection des programmes télédiffusés réservés à un public déterminé, n° 93), procédés du type de celui ayant donné lieu à l'arrêt précité du 19 août 1992 (cette *Revue,* p. 566). Mais il ressortait de ce dernier arrêt que l'emploi d'un procédé *quelconque* procurant à autrui l'accès à des programmes, en fraude des droits de l'exploitant du service, suffisait à caractériser ce délit ; il

avait été en outre relevé à cette occasion que le prévenu avait transmis mensuellement les codes de Canal Plus au gardien de l'ensemble immobilier où le piratage s'était produit, de manière à permettre la réinjection des programmes sur le réseau privé intérieur. La cour d'appel s'est donc bornée à en tirer les conséquences dans l'affaire ici étudiée.

Mots clés :
INFORMATIQUE * Piratage * Internet * Technologie