N° 3

SÉNAT

PREMIÈRE SESSION ORDINAIRE DE 1987-1988

Annexe au procès-verbal de la séance du 2 octobre 1987.

RAPPORT

FAIT

au nom de la commission des Lois constitutionnelles, de Législation, du Suffrage universel, du Règlement et d'Administration générale (1) *sur la proposition de loi* ADOPTÉE PAR L'ASSEMBLÉE NATIONALE, *relative à la* **fraude informatique,**

Par M. Jacques THYRAUD,

Sénateur.

(1) *Cette commission est composée de :* MM. Jacques Larché, *président ;* Félix Ciccolini, Charles de Cuttoli, Paul Girod, Louis Virapoullé, *vice-présidents ;* Germain Authie, René-Georges Laurin, Charles Lederman, Pierre Salvi, *secrétaires ;* MM. Guy Allouche, Alphonse Arzel, Gilbert Baumet, Christian Bonnet, Raymond Bouvier, Auguste Cazalet, Michel Charasse, Henri Collette, Raymond Courrière, Etienne Dailly, Michel Darras, Marcel Debarge, Luc Dejoie, Michel Dreyfus-Schmidt, Mme Jacqueline Fraysse-Cazalis, MM. François Giacobbi, Jean-Marie Girault, Jacques Grandon, Paul Graziani, Hubert Haenel, Daniel Hoeffel, Charles Jolibois, Bernard Laurent, Guy Malé, Paul Masson, Hubert Peyou, Albert Ramassamy, Roger Romani, Marcel Rudloff, Michel Rufin, Jacques Thyraud, Jean-Pierre Tizon.

Voir les numéros :

Assemblée nationale (8e législ.) : **352, 744** et T.A. **117.**
Sénat : 279 (1986-1987).

Droit pénal. – *Informatique.*

SOMMAIRE

Mesdames, Messieurs,

L'accroissement continu des capacités des systèmes de traitements automatisés de données et les perspectives ouvertes par les nouvelles techniques développées autour de l'informatique sont porteurs d'incontestables promesses, tant pour l'avenir de nos sociétés que pour l'existence quotidienne de chacun d'entre nous. Il est toutefois préoccupant de constater que l'extension des utilisations de l'informatique, la densification des réseaux et la multiplication des interconnexions ont donné naissance à de nouvelles formes de délinquance qui prennent aujourd'hui une ampleur considérable.

Soucieux d'attirer l'attention des pouvoirs publics, des entreprises et des citoyens sur la nécessité d'adopter un comportement responsable vis-à-vis des systèmes informatiques dont ils ont la gestion ou auxquels ils peuvent avoir accès et d'opposer aux auteurs de délits informatiques un dispositif pénal adapté à la répression de ces agissements frauduleux, M. Godfrain et plusieurs de ses collègues ont pris l'heureuse initiative de déposer à l'Assemblée nationale, en août 1986, une proposition de loi relative à la fraude informatique.

Le texte dont nous sommes aujourd'hui saisis est la version remaniée de cette proposition de loi, adoptée par l'Assemblée nationale au cours de la session de printemps, sur l'excellent rapport de M. le député René André.

La rédaction initiale de M. Godfrain a en effet été modifiée au cours des débats, afin de définir de nouvelles incriminations pénales susceptibles de sanctionner, en tant que tels, des agissements délictuels spécifiques dont les systèmes informatiques sont les objets, plutôt que d'étendre à l'informatique certaines incriminations préexistantes du code pénal.

S'il peut paraître paradoxal que ce soit par l'intermédiaire d'un texte à caractère pénal que l'informatique poursuive son insertion dans le champ juridique, il est en revanche incontestable que l'aggravation continue de la délinquance suscitée par le développement des techniques informatiques, requiert de toute urgence la mise en place d'un dispositif répressif adapté ; en effet, le juge pénal est tenu à une interprétation stricte des règles pénales et peut, de ce fait, en

l'absence de textes adaptés, se trouver dans l'incapacité de poursuivre des actes pourtant constitutifs de véritables "fraudes informatiques".

Le droit pénal en vigueur n'intéresse directement l'informatique que sur deux points particuliers : la protection des données personnelles, sanctionnée par la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et la protection des logiciels contre les opérations de contrefaçon, garantie par la loi du 3 juillet 1985 relative au droit d'auteur. Il convient, par conséquent, d'examiner puis de prolonger la réflexion engagée à l'Assemblée nationale, afin de doter notre société d'un droit mieux adapté à la répression des principales formes de délinquance informatique.

Avant de procéder à l'examen détaillé des dispositions qui nous sont soumises, on évoquera dans une première partie, les perspectives ouvertes par les développements de l'informatique et les nouvelles formes de délinquance qui menacent une société fragilisée par ces innovations technologiques ; dans un second temps, on analysera les réponses que le droit pénal apporte déjà pour une répression efficace de la délinquance informatique, tant en droit interne que dans ceux des Etats qui, sur ce point, ont adopté une législation spécifique.

PREMIERE PARTIE

LA VULNERABILITE DE LA SOCIETE INFORMATISEE

Si la collecte et le traitement de l'information ont toujours été des nécessités à toutes les époques, l'apparition de l'informatique au lendemain de la seconde guerre mondiale a marqué une étape importante, dans la mesure où le traitement de l'information par des moyens automatiques confère une nouvelle dimension à ces activités.

A. L'informatique emporte une véritable "révolution technologique"

Le développement des applications de l'informatique est un facteur de transformation de l'organisation économique et sociale et du mode de vie, dont toutes les conséquences n'ont pas encore été mesurées. L'importance de l'évolution dans laquelle nos sociétés sont ainsi engagées a conduit Simon Nora et Alain Minc à parler de "révolution technologique" (1). Leurs prévisions sur ce point se sont amplement réalisées.

. De l'informatique élitiste à l'informatique de grande diffusion

Il y a trente ans, l'informatique se présentait comme une science ésotérique dont l'accès était réservé à quelques techniciens privilégiés, seuls capables de percer l'hermétisme du langage machine et de l'assembleur. Les ordinateurs des premières années cinquante étaient composés de lampes et d'éléments électromécaniques encombrants et fragiles ; ils exigeaient des salles de calcul de bonnes dimensions, leurs capacités de mémoires étaient limitées à quelques dizaines de milliers de caractères et il leur fallait plusieurs millisecondes pour exécuter une opération en virgule flottante avec trente-deux chiffres de précision (2).

---

(1) S. Nora et A. Minc, L'informatisation de la société. Documentation française, janvier 1978.

(2) V. F. Sallé, Les ordinateurs, des ancêtres à la cinquième génération. Projet, août-septembre 1986, p. 6.

Aujourd'hui, une calculatrice programmable à piles offre des capacités et des performances bien supérieures à celles de ces antiques machines, tandis que les grands ordinateurs ont vu leurs capacités de mémoire de travail atteindre la centaine de millions de caractères, leurs fichiers stocker des centaines de milliards de caractères et leur vitesse de calcul se chiffrer en nanosecondes voire même en microsecondes (1).

L'apparition des **transistors** puis des **circuits intégrés** a permis une amélioration des coûts rapportés aux performances, une diminution du volume des installations et une fiabilité accrue des traitements. La mise au point d'une ligne de produits universels pour la gestion et le calcul scientifique s'est accompagnée du souci de rendre les différents **matériels compatibles** entre eux et d'une simplification des langages de programmation ; toutefois, au seuil des années soixante-dix, l'informatique restait isolée -toutes les machines étaient rassemblées dans le même lieu-, centralisée -toutes les informations remontaient des services utilisateurs- et réservée à une minorité -en France, en 1970, 250 entreprises possédaient 80 % du parc d'ordinateurs.

Des progrès importants ont marqué la décennie suivante, grâce à la **miniaturisation des composants électroniques** et au développement des **réseaux en temps réel** ; les anciennes rigidités se sont assouplies avec l'accroissement des capacités de stockage, les facilités d'accès aux systèmes et la programmation en un langage qui se rapproche sans cesse du langage naturel.

Aujourd'hui, l'informatique "explose" : une infinité de petites machines apparaissent, efficaces et peu coûteuses ; "à une technique élitiste, succède une activités de masse" (2). En outre, l'imbrication croissante des ordinateurs et des télécommunications, la **mutation des systèmes de télécommunications**, la numérisation du son et de l'image et les liaisons par satellites ouvrent un horizon radicalement neuf qui consacre la fin de la conception d'une technologie traditionnellement confinée dans son ghetto et fait définitivement perdre leurs allures démiurgiques aux relations entre l'homme et la machine.

---

(1) 1 nanoseconde = 1 millionième de seconde

1 microseconde — 1 milliardième de seconde

(2) S. Nora, A. Minc, rapport précité.

Demain, la miniaturisation toujours plus poussée des circuits intégrés accélèrera encore la vitesse de traitement ; les progrès conjoints des ordinateurs et des moyens de transmission permettront l'extension de réseaux d'échanges universels desservant ordinateurs professionnels et domestiques, et la simulation de certains mécanismes du raisonnement humain avec des ordinateurs de grande puissance ouvrira la voie au développement de réels **"systèmes experts"** : la planète pourrait alors prendre les allures de ce "village global" prophétisé par McLuhan? (1)

. L'informatique se répand dans tous les secteurs d'activité

Notre propos ne saurait être d'envisager ici une analyse des conséquences de cette mutation technologique. Il apparaît toutefois clairement que l'introduction de l'informatique dans la quasi-totalité des secteurs d'activité ne peut que contribuer à bouleverser les hiérarchies de micro-pouvoirs inhérentes à tout milieu professionnel (2) et les stratégies de macro-pouvoirs conduites par les groupes multinationaux, de même qu'elle risque de singulièrement modifier les modes de régulation de la société sur le plan mondial.

L'ordinateur est aujourd'hui présent aussi bien chez les ménages que dans les entreprises. **L'informatisation de masse,** qui a fait son apparition en 1978 avec les premiers micro-ordinateurs personnels, a franchi une nouvelle étape en 1985 avec l'implantation des **vidéotex** -le succès rencontré par le célèbre "minitel" français en est sans conteste la meilleure illustration (3). Les ménages ont accès à l'informatique de façon courante, que l'on songe aux lecteurs de disques compacts -une symphonie réduite à 600 millions de bits et reconvertie en temps réel par un processeur-, aux centraux téléphoniques numériques, aux distributeurs automatiques de billets (DAB) (4) et, demain, à la télévision à haute définition.

Les traitements automatisés de données, utilisés depuis longtemps pour le calcul scientifique, la gestion ou la documentation, sont aujourd'hui présents dans un nombre croissant de domaines, tels l'imagerie médicale, la photocomposition, le traitement de texte ou les machines à commandes numériques. La C.F.A.O. -conception et fabrication assistées par ordinateur- qui combine calcul scientifique automatisé, numérisation des images, automates et machines-outils,

---

(1) Marshall McLuhan, Pour comprendre les médias, Mame/Le Seuil, Tours et Paris, 1968, pp. 19-20.

(2) Voir, par exemple, Les partenaires sociaux face au changement technologique, B.I.T., Genève, 1986.

(3) Trois millions de minitels sont aujourd'hui installés ; le chiffre de cinq millions devrait être atteint en 1990.Par ce moyen, les foyers français ont accès à plus de 2 500 services.

(4) On compte actuellement plus de 9 000 DAB implantés dans toute la France.

est une technique qui permet, à distance, de concevoir et de réaliser de bout en bout de la chaîne de fabrication et de conditionnement, toute une série de produits industriels ; du bureau d'études à l'usine, il suffit aujourd'hui de quelques contrôleurs, souvent relayés par des satellites, pour veiller au bon déroulement d'opérations entièrement automatisées.

Le nombre des automates dont les programmes sont "gelés dans le silicium" est en rapide progression ; les produits intégrant la micro-électronique représentent aujourd'hui 40 à 70 % du chiffre d'affaires de secteur comme le travail des métaux, la construction mécanique, la construction de véhicules, la construction navale et aéronautique ou encore la construction électrique : "le matériel s'estompe, le logiciel se déploie" (1). L'informatique, dans sa version **"productique"**, est devenue le passage obligé de la modernisation de l'outil.

Dès l'école primaire, les enfants sont initiés aux nouvelles technologies -notamment dans le cadre du plan **"informatique pour tous"**- et une grande partie de la formation professionnelle est consacrée à l'acquisition ou au développement des connaissances des adultes dans ces domaines.

L'agence de l'informatique, créée en 1979, au lendemain du rapport Nora-Minc, a publié, en 1986, un état de l'informatisation de la France, d'où il appert que la valeur du parc français ne représentait en 1985 que 3 % du PIB, alors qu'elle atteignait 3,8 % en Grande-Bretagne et 4,4 % aux Etats-Unis (2). On notera, toutefois, que l'accélération du rythme des livraisons et l'apport représenté par les minitels ont maintenant probablement permis à la France de combler son retard.

Les taux d'informatisation observés en 1985 montraient une grande inégalité entre les secteurs : 30 à 60 % dans l'industrie, 60 à 80 % pour les experts-comptables, 57 % des entreprises de commerce en gros, mais seulement 5 % de l'hôtellerie, 1 % de l'agriculture et 0,5 % des médecins.

Dans le domaine des services, la profession bancaire est l'une de celles qui se sont le plus modernisées au cours de la dernière décennie ; l'innovation technologique, et plus particulièrement l'informatique, ont été des éléments déterminants de ce développement. Dès 1984, la banque représentait 18 % des dépenses informatiques en France, alors que son chiffre d'affaires n'excédait pas 3 % du PIB.

La caractéristique la plus frappante de l'utilisation de l'informatique par les banques est le rôle qu'y jouent les télécommunications, aussi bien dans les échanges internes aux établissements - téléinformatique, messagerie, documentation- que

---

(1) Allocution du Président de la République au colloque "Informatique et sécurité", 28 septembre 1979

(2) Rapport sur l'état d'informatisation de la France, 1979-1985, Paris 1986.

dans les relations avec les partenaires de la banque, qu'il s'agisse de la clientèle à laquelle sont proposés des services de télépaiement ou de vidéocomptes, ou qu'il s'agisse des réseaux informatiques financiers comme le système interbancaire de télécompensation (S.I.T.), le réseau interbancaire de paiement par carte (R.I.P.C.) ou le système SWIFT (1) mis en place dès 1977, qui permet le transfert électronique quotidien de plus de 600 milliards de dollars dans le monde entier (2).

Ces remarquables développements technologiques ne doivent pas masquer les risques inhérents au processus même d'informatisation : à bien des égards, la société informatisée est également une société de plus en plus vulnérable.

B. La société informatique est vulnérable

. La grande peur de l'an deux mil : l'ordinateur ?

Le développement des techniques informatiques, la centralisation des données personnelles, l'extension des réseaux et la vitesse de circulation des informations que l'informatique permet, constituent autant de menaces pour l'individu dont la liberté est comme encadrée par la somme des renseignements qui le concernent.

De même, le rôle croissant de l'ordinateur dans la vie quotidienne et dans la gestion de secteurs vitaux de l'économie ne peut manquer de préoccuper ceux qui ont le sentiment qu'à terme, ce n'est plus l'homme qui dominera la machine, mais la machine qui dominera l'homme.

Le spectre de la dictature de l'ordinateur alimente un nouveau millénarisme que George Orwell a illustré dans 1984 : "Big Brother is watching you", Big Brother vous regarde.

Certes, on peut penser avec la commission Chenot (3) que "l'informatique suscite aujourd'hui plus de craintes par ce qu'elle pourrait faire que par ce qu'elle fait réellement" et que ce phénomène "s'explique en partie par un certain mystère et par l'ampleur des ambitions de ceux qui sont les promoteurs de son emploi" ; il est toutefois préoccupant de constater que ces craintes ne sont pas l'apanage du seul "grand public" et que les spécialistes les partagent à bien des égards.

---

(1) SWIFT = Society for worldwide interbancary fund transfert, qui traite un million de virements internationaux par jour entre 1 000 banques situées dans 50 pays.

(2) P. Gillin, cité par André Bertrand, in Expertises, n° 62.

(3) Commission "Informatique et Libertés" présidée par M. Bernard Chenot dont le rapport, rédigé par M. Bernard Tricot, a été publié en juin 1975.

. Les inquiétudes des spécialistes

Les spécialistes des systèmes de traitements automatisés de données sont conscients de la **fragilité des mécanismes élémentaires** de l'informatique ; ils constatent qu'en raison de cette vulnérabilité, "l'ordinateur est source d'insécurité par la puissance qu'il développe, les biens informatiques sont en proie à l'insécurité par les convoitises qu'ils suscitent" (1).

La société informatisée vit dans une **dépendance accrue** vis-à-vis des grands systèmes ; or, il apparaît clairement que l'informatique n'est pas toujours sûre : le mythe de l'ordinateur infaillible a vécu.

Sans se livrer à une présentation détaillée des faiblesses des systèmes, il est néanmoins possible de rappeler que l'exactitude des données enregistrées dépend autant de la fiabilité des sources d'information et de la précision de la saisie que du bon fonctionnement des logiciels de traitement et des techniques de restitution des données.

Les pannes constituent également la source de difficultés majeures. C'est ainsi qu'une indisponibilité momentanée d'un système peut paralyser les cotations boursières ou les réservations de transports et occasionner de considérables préjudices (2). Le développement des micro-pannes a souvent conduit les concepteurs des systèmes à prévoir des sécurités internes : sauvegarde des travaux au fur et à mesure de leur exécution, doublement, voire triplement des capacités de traitement afin que la partie défaillante du système soit immédiatement relayée (3), détection préventive des pannes et télémaintenance ; ces procédures de sécurité sont toutefois coûteuses et l'intérêt économique ne les encourage pas toujours.

Le fonctionnement défectueux des systèmes constitue également un risque spécifique introduit par l'informatique ; sur ce point, la presse s'est fait l'écho de quelques affaires spectaculaires : une sonde spatiale égarée dans l'espace après que l'ordinateur eut confondu un point et une virgule, vingt mille pots de yaourth perdus en quelques minutes à la suite d'un incident de fabrication dans la chaîne automatisée de production, autant d'exemples qui illustrent la fragilité de ces systèmes.

---

(1) J. Chamoux - Menaces sur l'ordinateur - Le Seuil 1986.

(2) A Sochaux, chez Peugeot, une heure de panne du système informatisé correspondrait à la perte de cent voitures (soit 4 millions de francs, chiffre cité par Yves Lasfargue dans "De la peine à la panne", Le Monde, 22 août 1987).

(3) Technique dite de la "redondance", c'est-à-dire de la tolérance intégrée aux pannes : chaque composant est multiplié plusieurs fois et la fiabilité s'accroît d'autant.

Plus les systèmes automatisés sont récents, plus ils sont intégrés, c'est-à-dire que les machines dépendent de plus en plus les unes des autres. De ce fait, les systèmes "hautement intégrés", tels les ateliers robotisés ou les réseaux de télécommunications, sont les plus fragiles. C'est en ce sens que l'on a pu écrire que l'évolution qui s'amorce ainsi nous conduit de "la civilisation de la peine (travaux physiques à effectuer) à la civilisation de la panne, où les travaux principaux sont des travaux de surveillance, de maintenance, de diagnostic et de dépannage" (1).

A cette vulnérabilité spécifique de la société informatisée qui découle de la fragilité des systèmes et des défaillances des traitements, s'ajoute un autre risque qui est au centre des préoccupations des auteurs du texte qui vous est soumis : **la fragilité interne des systèmes facilite le développement d'une nouvelle délinquance** prompte à utiliser les failles et les faiblesses de ces systèmes afin de servir la cupidité, les ambitions économico-stratégiques ou le goût du pouvoir de ses promoteurs.

Les enjeux de la sécurité informatique apparaissent considérables et l'un des mérites de la proposition de loi de M. Godfrain est d'attirer l'attention de tous ceux qui sont en relation avec l'informatique sur les risques spécifiques que son utilisation fait courir aux personnes, aux entreprises, aux services, aux économies nationales, à la sécurité des Etats, aux relations économiques, financières et politiques internationales.

Le problème clé de la sécurité informatique est un **problème technique** ; c'est également un **problème de comportement, de moeurs, de société** ; c'est pourquoi "il faut une réponse juridique qui officialise le mal et encadre la réaction sociale" (2).

C. L'informatisation de la société a suscité une nouvelle délinquance

. L'ampleur du phénomène est difficile à appréhender

Dès 1975, le rapport Tricot soulignait que l'informatique faisait naître de nouvelles craintes qui, à certains égards, devaient de se révéler fondées ; quelques années plus tard, en 1978, le ministère de la défense suédois publiait le rapport du comité SARK, intitulé "la vulné-

---

(1) Yves Lasfargue, article précité.

(2) Jean Devèze, La fraude informatique - Aspects juridiques, la semaine juridique, Ed. E n° 31/33 13 août 1987, p. 15 000..

rabilité de la société informatisée" (1) et l'année suivante, en 1979, le rapport de Genève alertait les entreprises en leur démontrant que l'utilisation de l'informatique leur faisait courir des risques spécifiques.

Sensibilisé au problème, le Gouvernement français a récemment mis en place une délégation interministérielle pour la sécurité des systèmes d'information, chargée de coordonner les politiques des différentes administrations en la matière ; cette délégation est complétée par une instance de concertation dénommée commission interministérielle pour la sécurité des systèmes d'information et par un service central de la sécurité des systèmes d'information composé d'experts techniques.

S'il semble que les responsables économiques et politiques soient aujourd'hui sensibilisés à ce que l'on désigne communément sous le vocable de "fraude informatique", il apparaît en revanche que "la criminologie de la délinquance informatique est encore dans les limbes" (2) et qu'aucune statistique vraiment pertinente n'ait pu être établie.

Cette situation s'explique par plusieurs raisons dont les principales sont **l'absence d'incriminations pénales spécifiques permettant d'alimenter les catégories statistiques correspondantes**, et la difficulté à identifier des cas précis en raison du **silence des victimes** qui craignent que ne soit porté atteinte à leur crédibilité commerciale et doutent de l'efficacité de l'action de la police et de la justice car il est souvent difficile d'apporter les preuves matérielles des infractions commises. C'est ainsi que l'américain Don Parker, l'un des pionniers de la recherche criminologique sur les "computer abuses", estime qu'aux Etats-Unis, seules 20 à 25 % des fraudes sont effectivement signalées (3).

On note, toutefois, un souci croissant de la part des services de police et des pouvoirs publics d'obtenir des renseignements plus précis ; c'est ainsi que certains pays s'efforcent de centraliser l'information et font obligation aux entreprises de déclarer les fraudes dont elles ont été victimes. En Autriche, le directeur adjoint du centre d'informatique du ministère de l'Intérieur est expert en matière de délinquance informatique ; à ce titre, il est chargé d'examiner tous les cas de fraude liés à l'informatique qui lui sont signalés.

---

(1) "The Vulnerability of the computerised society" pour l'édition anglaise publiée en 1979

(2) Raymond Gassin, Le droit pénal de l'informatique, D. 1986,Chr. V, p. 35.

(3) Don Parker, Crime by computer, New York 1976, pour le Stanford research institute.

En France, où en l'absence de législation répressive spécifique, il n'existe ni obligation de déclaration, ni centralisation systématique des informations, la police judiciaire dispose néanmoins d'un service spécialisé dans les affaires de fraude informatique, chargé, le cas échéant, de conseiller les autres services de police confrontés à des faits en relation avec l'informatique et, par le moyen de questionnaires adressés à ces services, d'établir des références statistiques pour les années récentes. Les personnels de ce service ont bénéficié d'une formation technique appropriée destinée à leur permettre d'enquêter dans les systèmes informatiques afin d'y repérer les indices et les preuves des délits commis.

Si les administrations commencent seulement à se préoccuper de mesurer l'ampleur du phénomène, les universités, en revanche, conduisent des travaux sur le sujet depuis le début des années 1970, soit pour alimenter les réflexions des pénalistes, soit pour fournir des informations précises à certains organismes dont les adhérents sont les victimes désignées de ces agissements frauduleux, telles les banques, les compagnies d'assurances ou les entreprises du secteur informatique. C'est ainsi qu'ont été conduites, au moyen de questionnaires, les premières investigations du Caulfield institute of technology australien, du centre de droit pénal international belge, du Stanford research institute de Californie ou de l'institut de criminologie et de droit pénal économique de l'Albert Ludwigs universität de Fribourg-en-Brisgau.

En France, l'Association du droit de l'informatique créée en janvier 1985, s'est également livrée à des études sur la fraude informatique qui lui ont pemis de conduire de très intéressantes réflexions sur les réponses qu'en la matière le droit apporte, ou est susceptible d'apporter.

Les compagnies d'assurances se sont également intéressées à la fraude informatique qui représente pour elles un risque élevé de sinistres, lourd de menaces de coûts supplémentaires pour l'avenir. C'est ainsi qu'en France l'A.P.S.A.I.R.D. (Association plénière des sociétés d'assurance contre l'incendie et les risques divers) a procédé à une première enquête sur l'année 1984.

Enfin, dans plusieurs pays, des colloques se tiennent chaque année, qui réunissent des spécialistes de la fraude informatique, afin qu'ils puissent confronter leurs expériences et grâce aux études de cas qu'ils rassemblent, mettre au point des parades contre des délinquants toujours plus inventifs.

. L'évolution du coût des sinistres suit une croissance géométrique.

Les fraudes informatiques causent des préjudices considérables dont les plus évidents atteignent principalement les banques (1), les établissements de crédit et les compagnies d'assurances. En dépit des imperfections des données statistiques disponibles, il apparaît clairement que le coût moyen global des sinistres informatiques liés à la fraude croît rapidement d'une année sur l'autre et les estimations les plus raisonnables avancent **un doublement des coûts chaque année.** C'est ainsi que l'A.P.S.A.I.R.D. a estimé que les fraudes, sabotages ou indiscrétions qui représentaient en 1984 **13 % des pertes engendrées par les sinistres informatiques,** constituaient pour l'avenir le risque potentiel le plus menaçant et le plus coûteux.

En effet, si ce chiffre de 13 % paraît encore modéré au regard des conséquences des erreurs de saisie et d'utilisation (32 % des pertes), des accidents entrainant la destruction partielle ou totale des matériels (20 %), des erreurs de conception, de réalisation ou d'exploitation (19 %) et des pannes de matériel ou de logiciels (17 %), il est toutefois préoccupant de constater que l'étude conduite en France par la police judiciaire montre que le nombre des délits recensés double chaque année depuis 1981, que le montant moyen du préjudice financier s'élève à 2,2 millions de francs et que pour la seule année 1986, il a été recensé autant de délits que sur l'ensemble de la période 1981-1985 (2).

En 1984, des estimations américaines évaluaient le coût global de la fraude informatique à 100 millions de dollars pour les seuls Etats-Unis et à 30 millions de dollars pour le Japon (3) ; la France est encore éloignée de ces chiffres, mais le rythme de progression de la délinquance laisse présager des résultats comparables d'ici à quelques années.

S'il apparaît difficile d'obtenir des statistiques précises sur le phénomène de la délinquance informatique, il est toutefois clair que l'ensemble des études menées dans les différents pays démontre que ces nouvelles formes de délinquance sont en pleine expansion.

Les analyses prospectives conduites aux Etats-Unis ou en Allemagne font valoir que, comme en France, le développement de cette délinquance y suit une progression d'allure géométrique, même s'il est probable que cette évolution n'est pas totalement imputable à un accroissement subit de la délinquance et qu'elle s'explique également par une meilleure appréhension des phénomènes de fraude de la part

---

(1) Les banques viennent en tête des secteurs victimes de la fraude informatique. V. les travaux du Stanford research institute cités in François Guérin, Maîtriser l'informatique, Delmas 1984.

(2) Ces chiffres ne sont pas exhaustifs ; les statistiques portent sur les 72 cas recensés pour la période 1981-1986.

(3) V. Computer world 1984, n° 45 et n° 52.

des services de police ou des sociétés d'assurance ; de même, l'idée selon laquelle plus les années passent, plus les fraudes sont techniques, n'est-elle pas véritablement significative d'une évolution de la délinquance elle-même et de l'habileté croissante de ses auteurs, mais bien plutôt la marque d'une amélioration de la détection des fraudes et de la qualité des statistiques disponibles.

On relèvera par ailleurs que **certains préjudices sont difficilement évaluables**, notamment lorsqu'il n'y a eu aucune manipulation de données ou de traitements ; en effet, en pareils cas, c'est l'information contenue dans le système qui fait l'objet d'une diffusion à des personnes non autorisées : **or, si l'information en tant que telle n'est pas pour l'heure un bien susceptible de bénéficier d'une véritable protection juridique (1), elle présente en revanche toutes les caractéristiques d'une valeur patrimoniale (2) qui peut se trouver amoindrie ou même totalement dévaluée par une diffusion excessive.**

. De nouvelles formes de délinquance "en col blanc"

Le développement de l'informatique, comme sans doute l'apparition de toute nouvelle technologie, a suscité la naissance, puis l'épanouissement, de formes spécifiques de délinquance, promptes à détourner l'informatique de ses objets, afin d'en tirer un bénéfice, ou habiles à faire montre d'une grande ingéniosité susceptible de conforter une image de compétence.

Si plusieurs motivations peuvent expliquer le phénomène de la fraude informatique, il est toutefois frappant de constater que l'image traditionnelle du "hacker", c'est-à-dire de l'adolescent fasciné par l'informatique qui essaie, dans un dessein purement ludique, de s'introduire dans des systèmes informatiques afin de faire la preuve de son habileté, ne représente plus aujourd'hui le principal milieu de recrutement de cette nouvelle délinquance.

Les clubs de passionnés de l'informatique sont certes légions ; popularisés par le film "War game", ces "bricoleurs de génie" peuvent se révéler redoutablement efficaces ainsi qu'en témoignent les récents succès du Chaos Computer Club (C.C.C.) de Hambourg qui aurait réussi, de l'aveu même de ses dirigeants, à pénétrer le réseau

---

(1) "L'information reste une notion aux contours imprécis dont la nature est incertaine". V. M.P. Lucas de Leyssac, L'information est elle un bien susceptible de vol ou d'une autre atteinte juridique aux biens ? D. 1985, Chr. IX, p. 43.

(2) V. P. Catala, Ebauche d'une théorie juridique de l'information, D. 1984, Chr. XVII, p. 97.

informatique international SPAN (Space Physics Analysis Network), construit par la NASA, l'agence spaciale américaine, ainsi que certains fichiers du CEA, le commissariat à l'énergie atomique (1).

On notera que d'une façon générale, **les "hackers" se contentent de jouer les "voyeurs"** dans les systèmes qu'ils pénètrent ; ils les survolent sans détruire ni modifier les données ou les programmes. La prolifération de ces clubs reste toutefois préoccupante dans la mesure où la divulgation de certaines informations peut causer de graves préjudices, par exemple lorsque, par ce moyen, des informations concernant **la défense nationale** ou les intérêts vitaux du pays viennent à être rendues publiques (2) ; elle est également inquiétante, dans la mesure où elle permet la mise en commun et la gestion rationnalisée de compétences qui, une fois rassemblées, offrent à leurs détenteurs de considérables moyens de pression, voire même de chantage.

Une étude américaine, rédigée en 1986 par le directeur du N.C.C.C.D. (National center for computer crime data), montre que 13 % des "computer crimes" retenus sont le fait d'"étudiants", à l'instar de ce "groupe des 414" qui, à Milwaukee, en 1983, a pénétré différents systèmes bancaires. Mais les véritables délinquants, poursuit cette étude, se recrutent en fait en dehors de ces milieux.

C'est ainsi que l'enquête conduite par la police judiciaire française souligne qu'en termes de préjudices, les fraudes commises par des personnes appartenant -ou ayant appartenu- à l'entreprise victime d'un **piratage** représentent actuellement plus de 77 % des fraudes recensées (68 % des préjudices), qu'il s'agisse **des employés** (52,8 % des fraudes et 15,3 % des préjudices) **ou des cadres et des dirigeants** (25 % des fraudes et 52,8 % des préjudices). L'étude précitée du N.C.C.C.D. vient confirmer ces résultats et mettre en relief le rôle prépondérant des services informatiques dans les fraudes détectées.

De multiples exemples pourraient illustrer les techniques utilisées par les délinquants ; c'est ainsi que l'on peut évoquer le cas de cet employé d'une Caisse d'épargne de Rennes qui, après avoir repéré les comptes qui n'effectuaient que des opérations épisodiques, s'en est servi pour simuler des retraits à son seul profit. De 1974 à 1978, il put ainsi masquer ses malversations en contrepassant le solde réel au moment où le client se présentait, grâce à des prélèvements opérés sur

---

(1) V. International Herald Tribune du 17 septembre 1987 "Hambourg hackers say they got NASA secrets".

(2)V. B. Warusfeld, Sécurité informatique et secret défense. Défense nationale, février 1986, p. 83.

d'autres comptes, destinés à garantir une "balance carrée" des soldes enregistrés en caisse. L'escroquerie ainsi réalisée a rapporté à son auteur une somme totale d'environ 340 000 francs... et cinq ans de prison ! (1)

Le piratage peut revêtir de multiples aspects : **création de données inexactes** -aux Etats-Unis, plusieurs milliers d'électeurs fictifs ont ainsi été introduits dans les fichiers électoraux de divers comtés-, **modification ou annulation de données** -le fichier des contraventions de la ville de Dallas a été partiellement effacé-, **modification des programmes de traitement** par l'introduction de "boucles" permettant par exemple de créditer un compte de tous les centimes éliminés dans les calculs d'intérêts bancaires (2).

En 1983, sur les 150 cas recensés de fraudes importantes effectuées par action sur les traitements, Brandt Allen déterminait comme suit leur importance relative (3) :

- Ajout ou modification de transactions :	65 %
- Modifications de fichiers :	8 %
- Transactions supprimées :	4 %
- Altération des programmes :	9 %
- Utilisations incorrectes :	3 %
- Autres :	11 %

Dans certains cas de vengeance, les fraudeurs peuvent également se livrer à de véritables opérations de **sabotage** par destruction, soit immédiate, soit progressive -la technique dite du "virus"-, des données ou des traitements ; cependant, il résulte clairement des travaux d'étude disponibles que, le plus souvent, le principal but poursuivi par le délinquant, surtout lorsqu'il est extérieur à l'entreprise, est de détourner des fonds ; l'une des cibles privilégiées de ces détournements de fonds reste d'ailleurs les distributeurs automatiques de billets.

A ce propos, on peut s'interroger sur le caractère "informatique" des délits dont les **cartes bancaires** sont les instruments ; la multiplication actuelle des fausses cartes -environ 500 par mois- cause un préjudice considérable aux banques (11,5 millions de francs pour

---

(1) Cité in J.P. Chamoux, Menaces sur l'ordinateur, Le Seuil 1986.

(2) Technique dite du "salami".

(3) Chiffres cités par F. Guérin in Maîtrise l'informatique, Delmas 1984.

1986 (1)), mais il convient de distinguer entre les cas où la carte falsifiée, réencodée ou associée à des codes générés à cet effet, est un moyen frauduleux d'accès au système et doit, de ce fait, être considérée comme le moyen de commettre une fraude informatique, et les cas où la carte n'est qu'un instrument de paiement falsifié. On considèrera en conséquence que la **carte est un élément du système lorsqu'elle permet un accès direct à celui-ci.**

La future carte à micro-processeur, baptisée "carte à puce", comportera une mémoire de données ainsi qu'un micro-processeur qui, outre le contrôle d'accès à la mémoire, sera capable de gérer toutes les entrées-sorties de données et de mettre en oeuvre des algorithmes (chiffrement et déchiffrement de données par exemple) ; cette carte fera sans conteste partie intégrante du système de traitement, elle permettra également de renforcer la sécurité informatique des banques.

. Les ramifications internationales de la délinquance

L'internationalisation des communications informatiques se poursuit à un rythme accéléré, poussée par les besoins particuliers de certaines catégories d'agents économiques comme les firmes transnationales et les institutions financières (2).

L'affaire du "chaos computer club" évoquée plus haut, constitue une bonne illustration **des fraudes très complexes** que ce processus peut engendrer et montre comment, à partir d'un système peu ou mal protégé, il est possible d'accéder à un autre système et ainsi de suite par opérations successives dans tous les pays du monde, jusqu'à atteindre des cibles très protégées.

Ainsi, se pose aux Etats un problème de sécurité, car **il est très difficile de se protéger juridiquement et techniquement contre des actes de piratage commis hors des frontières** (3). **La coopération policière et judiciaire internationale** permet toutefois de renforcer l'efficacité des recherches et des poursuites (4) (5).

---

(1) Chiffre avancé, pour les banques françaises, par l'association française des banques (AFB)

.(2) Plus de 2 000 banques de données accessibles en 1985 contre environ 500 en 1979.

(3) L'article 693 du code de procédure pénale répute "commise sur le territoire de la République toute infraction dont un acte caractérisant un de ses éléments constitutifs a été accompli en France".

(4) V. par exemple la convention européenne d'entraide judiciaire du 20 avril 1959, ratifiée par la France le 23 juillet 1967.

(5) V. les travaux en cours au Conseil de l'Europe sur la fraude informatique. Voir également les travaux précités de l'OCDE et de la CCI.

La dimension internationale introduit également une nouvelle difficulté touchant à la souveraineté des Etats. Nombre d'entre eux craignent de voir leur "potentiel informationnel" -statistiques, brevets, données financières et économiques- aspiré par les réseaux internationaux de données et redoutent de perdre ainsi l'un des attributs de leur souveraineté. Ces réflexions qui posent d'ailleurs, sous une autre forme, la question du statut de l'information, conduisent certains Etats à jalousement protéger un ensemble croissant d'informations (1) et d'autres à réclamer la mise en place d'un **nouvel ordre mondial de l'information** (2).

Cette tension entre la souveraineté des Etats et la liberté de l'information en matière de flux transfrontières de données est un point sensible des relations internationales et elle rend plus difficile la mise en place d'une coopération internatinale en matière de lutte contre la fraude informatique, dans un contexte de solidarité technique de fait imposé par le développement des réseaux internationaux de communications.

. L'établissement d'une typologie des fraudes conditionne la définition du champ à criminaliser

Sans dresser un panorama complet des différents types de fraude, il n'est pas inutile de proposer une classification des fraudes constatées, afin d'établir clairement le rôle de l'ordinateur dans l'infraction et de déterminer les fraudes qui, en l'état actuel du droit, n'entrent dans le cadre d'aucune incrimination pénale.

Une telle démarche permettra, en effet, de définir avec précision les agissements que l'on entend sanctionner et évitera de faire double emploi avec d'autres dispositions du code pénal déjà applicables -et d'ailleurs appliquées à ce titre par la jurisprudence- à certains cas d'espèce plus ou moins rattachés à l'informatique.

La plupart des auteurs (3) s'accordent pour distinguer trois grandes catégories de délits au regard de la place qu'occupe l'informatique dans la structure concrète de l'acte infractionnel :

---

(1) V.A. Bertrand L'exportation illicite d'ordinateurs et de logiciels américains vers les pays de l'Est - Expertises n° 59.

(2) Cette notion a été développée dans le rapport de Sean MacBride pour l'Unesco, intitulé "Voix multiples, un seul monde", Documentation française, 1980.

(3) Voir notamment R. Gassin, Le droit pénal de l'informatique, D. 1986, Chr. V, p. 35 et J. Devèze, La fraude informatique - Aspects juridiques - La semaine juridique, éd. E n° 31/33, 13 août 1987.

- les cas dans lesquels **l'informatique est l'objet même de la délinquance** ;

- les cas dans lesquels **l'informatique est l'instrument, le moyen de la fraude** ;

- les cas dans lesquels **l'informatique fournit l'occasion de délits.**

L'informatique est l'objet même de la délinquance en cas de **sabotage matériel** des systèmes, tels ces "attentats technologiques" commis par le CLODO (Comité liquidant ou détournant les ordinateurs) ou encore en cas de **"piratage"**, soit qu'un usage non autorisé du système permette d'en détourner les capacités au bénéfice du fraudeur -ce "vol d'usage" est qualifié de **"vol de temps-machine"**-, soit que le délinquant s'approprie frauduleusement des logiciels ou des données ou qu'il en modifie le contenu.

L'informatique n'est que le moyen de commettre des délits, lorsqu'instrument actif de l'infraction, elle permet d'obtenir des sommes indues, de même, lorsqu'instrument passif de la fraude, elle permet au titulaire d'un carte bancaire de prélever dans un distributeur de billets une somme excédant le solde de son compte

Enfin, l'informatique est présente dans certains délits, par exemple à l'occasion de la vente de produits informatiques (1).

En l'absence d'un consensus entre les pays membres, les experts de l'O.C.D.E. se sont mis d'accord sur une "définition de travail" qui considère que "l'abus informatique est tout comportement illégal ou contraire à l'éthique ou non autorisé, qui concerne un traitement automatique de données et/ou une transmission de données" (2). En conclusion de son étude, **l'O.C.D.E.** propose de retenir comme fraudes informatiques :

- les manipulations informatiques ;

- l'espionnage par ordinateur ;

- le sabotage informatique ;

- le vol de temps ordinateur ;

- le détournement de fonds par utilisation de moyens informatiques ;

- l'accès indu aux systèmes et aux réseaux.

---

(1) Voir le conflit entre la CEE et IBM à propos des pratiques anti-concurrentielles de cette dernière au regard des articles 85 et 86 du traité de Rome.

(2) Politiques d'information, d'informatique et de communications : la fraude liée à l'informatique, analyse des politiques juridiques, OCDE 1986.

On relèvera d'ores et déjà que cette approche conduit aussi bien à l'incrimination de certains résultats frauduleusement obtenus (le détournement de fonds) qu'à la sanction, quelle qu'en soit l'issue, d'agissements spécifiquement informatiques (l'accès indu aux systèmes et réseaux) ; cette démarche est peut-être susceptible de conduire à une certaine confusion juridique sur laquelle il conviendra de s'interroger après avoir dressé le bilan des incriminations pénales dont dispose le droit en vigueur pour affronter la fraude informatique.

SECONDE PARTIE

LES REPONSES JURIDIQUES A LA DELINQUANCE INFORMATIQUE

A. Le droit pénal traditionnel permet déjà de réprimer certains délits informatiques

Avant même d'envisager la création d'infractions pénales spécifiques en matière de fraude informatique, il convient d'examiner si le droit pénal ne permet pas déjà d'incriminer un certain nombre d'agissements frauduleux dont l'informatique est soit le moyen, soit l'objet.

. Les délits commis grâce à la manipulation ou avec l'aide d'un ordinateur

On peut **définir** une première catégorie de délits **par le résultat obtenu** : les données ou les logiciels sont manipulés dans l'intention d'obtenir un bénéfice illicite, d'influencer des décisions ou de causer tout autre dommage à un ou plusieurs tiers.

Certes, **la catégorie de délits ainsi définie par l'intention de causer un tort n'emporte pas l'incrimination pénale de la manipulation elle-même, mais elle permet néanmoins de sanctionner le résultat illicitement obtenu par ce moyen.**

Les exemples de données informatisées susceptibles de faire l'objet de telles manipulations comprennent les transactions électroniques de transferts de fonds, les enregistrements des bases de donées des comptes bancaires ou d'épargne, les enregistrements des sommes à encaisser, les dossiers personnels et médicaux, les comptes d'heures de travail, les versements de salaires... Que la fraude consiste en une manipulation ou une création de données ou encore en une altération des programmes de traitement de ces données, **le parallèle avec la fraude non associée à l'informatique s'avère souvent aisé** et les auteurs de tels délits peuvent être poursuivis sans difficulté, notamment sur le fondement de l'**escroquerie**, du **faux et usage de faux**, du **vol** ou de l'**abus de confiance**, de l'**espionnage économique.**

C'est ainsi que la jurisprudence n'a pas hésité à qualifier d'escroquerie au sens de l'article 405 du code pénal, la remise de

sommes indues consécutives à la production de fausses factures traitées par ordinateur -les documents élaborés par ordinateur sont en effet "...de nature à persuader d'un crédit imaginaire dès lors qu'ils émanent d'un procédé électronique de calcul et de gestion donnant force de crédit" (1).

Se rend également coupable d'escroquerie la personne qui, en faisant usage d'un faux et en utilisant une carte magnétique dérobée, a procédé à des retraits d'argent dans un distributeur automatique de billets (2 et 3). En revanche, la jurisprudence se refuse à réprimer le titulaire du compte qui, au moyen de sa carte de crédit, retire de la billeterie une somme supérieure au montant de sa provision, dans la mesure où ce geste ne constitue que l'inobservation d'une obligation contractuelle (4).

Sans multiplier les exemples, on peut toutefois constater que le droit pénal, au moins pour certaines infractions, ne laisse pas le juge (et les victimes) totalement démuni (5).

Dans la plupart des pays, les cas de manipulations d'ordinateurs qui jusqu'à présent ont fait l'objet de poursuites pénales, ont pu être sanctionnés en vertu de telles dispositions (6). Il apparaît cependant que l'interprétation stricte de la règle pénale qui s'impose au juge répressif prévient souvent l'incrimination de l'agissement frauduleux qui a conditionné le délit, quand elle n'en empêche pas totalement la sanction. Ainsi en est-il souvent des trois autres catégories de délits que nous avons retenues : l'altération ou la destruction de systèmes informatisés, l'utilisation non autorisée d'un système de traitements ou de télécommunications, l'accès non autorisé à l'information.

. Les délits emportant l'altération ou la destruction de données ou de systèmes informatisés

Une information de grande importance pour une organisation peut se trouver privée de toute valeur si elle est totalement ou même

---

(1) Cass. Crim. 21 mars 1976, Bull. crim. n° 97, p. 232.

(2) Cour d'appel de Bordeaux, 25 mars 1987, D. 1987 - 424, note Breton.

(3) On notera qu'en matière d'usage de fausses cartes ou de cartes volées, les juges écartent la qualification de vol avec usage de clé volée.

(4) Cass. Crim. 24 novembre 1983, D. 1984 - 465, note Lucas de Leyssac.

(5) Voir X. Linant de Bellefond et A. Hollande, Droit de l'informatique, chap. F. droit pénal de l'informatique, p. 99. Delmas, 1984

(6) Chambre de commerce internationale, rapport de la commission des politiques de l'informatique, des télécommunications et de l'information relatif à "la délinquance contre l'information et les systèmes d'information : le point de vue de la communauté économique internationale", 15 juillet 1986, p. 8..

partiellement effacée ou altérée. La technique utilisée peut atteindre n'importe quel élément de l'infrastructure d'information : les mécanismes nécessaires à la conservation des données (par exemple les systèmes de gestion des bases de données), à l'accès (par exemple les canaux d'information, les dispositifs et les supports de stockage) et à la remise de l'information à ses destinataires (par exemple les réseaux de télécommunications).

Or, il s'avère qu'**hormi les cas de destruction physique des matériels** punis par les articles R 38-6° (détériorations mineures) 434, 435 et 437 du code pénal, **les dommages ainsi causés** que d'aucuns n'hésitent pas à qualifier de "délits contre l'information", **échappent au champ du droit pénal** qui, au moins en France, ne reconnaît pas à l'information le statut de "chose" au sens de l'article 379 du code pénal (1).

. *Les délits caractérisés par l'utilisation non autorisée d'un système de traitement ou de télécommunications*

Le droit pénal traditionnel n'apporte pas de réponse à ce que les informaticiens appellent "le vol de temps machine" ; il semble en effet que le vol (en fait vol d'usage) appliqué à l'occasion de l'emprunt d'un véhicule ne puisse être retenu en l'**absence de soustraction même momentanée de la chose**

On relèvera par ailleurs que la définition de l'utilisation non autorisée suppose que les **systèmes** soient **protégés** et que le délinquant ait violé les **mesures de sécurité.**

Les exemples d'utilisations non autorisées comprennent aussi bien l'usage abusif du système par des utilisateurs autorisés, que l'utilisation de capacités de traitements fermées au public, par des tiers non autorisés.

Outre les difficultés suscitées par la notion de système protégé, une incertitude apparaît également autour de l'utilisation autorisée dans la mesure où **l'habilitation d'un utilisateur trouve son fondement dans les relations contractuelles** que celui-ci entretient avec le maître du système ; **or, il est malaisé et sans doute inopportun de faire dépendre la constitution d'une infraction de liens contractuels.**

Ces deux difficultés doivent être élucidées dans le cadre de la mise au point d'un dispositif pénal adapté à la répression d'une catégorie de délits qui échappe au champ des incriminations traditionnellement retenues dans notre droit.

---

(1) "Quiconque a soustrait frauduleusement une chose qui ne lui appartient pas est coupable de vol".

. Les délits d'accès non autorisé à l'information

Des informations particulièrement sensibles ou confidentielles sont souvent traitées par ordinateur et transmises par les systèmes de télécommunications ; or, la divulgation de telles informations pouvant être préjudiciable, l'accès non autorisé à ces informations devrait être en lui-même considéré comme constitutif d'un délit.

Le droit français n'incrimine de tels comportements que dans les cas, clairement établis, où il existe un droit exclusif d'utilisation de l'information, par exemple au moyen des dispositions relatives à la protection des secrets de fabrique, du droit d'auteur ou encore du secret défense.

La protection de l'information par le **droit des propriétés intellectuelles** -droit d'auteur, brevet et marque- est partiellement applicable à l'informatique ; son efficacité dans le cadre qui nous préoccupe, se trouve considérablement limitée par le fait que **ce n'est pas l'information à l'état pur qui est ainsi protégée, mais seulement sa formalisation** (1).

Toute autre, en revanche, est **la protection assurée par le secret** ; elle **emporte** en effet, **l'interdiction de la révélation, de la reproduction ou de l'utilisation de l'information elle-même.** Sont par exemple opposables en l'espèce : le secret défense, le secret des correspondances, le secret professionnel, le secret de la vie privée, le secret des affaires... On notera toutefois que dans certains cas, seules les protections civile ou quasi-délictuelle sont retenues. On soulignera également que la portée des incriminations peut se trouver limitée ; c'est ainsi que seul le professionnel astreint au secret est coupable de délit de violation du secret professionnel (art. 378 du code pénal).

Au terme de ce rapide survol, on constate que le droit pénal traditionnel n'apporte pas de réponses suffisantes à tous les cas de délits informatiques recensés ; or, l'idée d'une législation spécifique a déjà fait l'objet de réflexions et de résultats qu'il convient d'examiner avec attention.

---

(1) L'adaptation législative du droit d'auteur aux logiciels a été réalisée dans un certain nombre de pays. V. infra le chapitre B.

B. Quelques dispositions pénales récentes sanctionnent d'ores et déjà des délits informatiques .

Dans un certain nombre d'Etats, des lois nouvellement promulguées sont venues sanctionner certains délits spécifiquement informatiques. Ces textes, qui ne couvrent que très imparfaitement le champ ouvert à la criminalité informatique, concernent deux aspects particuliers : **la contrefaçon de logiciels et la protection des données personnelles.**

Dans ces domaines, la France n'est pas demeurée en reste, et l'on peut même considérer, à certains égards, qu'elle a joué un rôle pionnier dont de nombreux pays se sont inspirés.

Ces textes constituent les premiers éléments de réflexion juridique dont nous disposons ; on nous pardonnera donc d'en présenter une analyse quelque peu détaillée.

. La protection pénale des personnes en matière de traitements informatiques nominatifs

Le droit en vigueur comporte un ensemble de textes spéciaux dont l'objet commun est de définir la place et le rôle de l'informatique au regard de la vie des citoyens et d'organiser une protection juridique des personnes à l'égard des traitements informatiques nominatifs.

La **loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés** constitue le texte le plus important de ce dispositif spécialisé dont font également partie la loi n° 80-2 du 4 janvier 1980 relative à l'automatisation du casier judiciaire, la loi n° 86-1305 du 23 décembre 1986 portant modification de la loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière statistique, la loi n° 70-539 du 24 juin 1970 sur la centralisation de la documentation relative à la circulation routière et l'article 25 de la loi n° 78-22 du 10 janvier 1978 relative à l'information et à la protection des consommateurs dans le domaine de certaines opérations de crédit.

Ces textes définissent une série d'incriminations pénales destinées à sanctionner le non respect des dispositions de droit substantiel qu'ils posent.

- Les personnes bénéficient d'une protection juridique spécifique à l'égard des traitements automatisés d'informations nominatives.

Conscients des menaces que l'informatique est susceptible de faire peser sur les libertés individuelles et le secret de la vie privée, les droits nationaux des pays occidentaux et le droit international se sont préoccupés d'apporter aux citoyens une protection juridique adaptée. A cet égard, la loi du 6 janvier 1978 s'ordonne autour de deux principes :

. L'emploi de traitements automatisés d'informations nominatives dans l'élaboration des décisions est très strictement encadré et les informations ainsi utilisées doivent être accessibles et contestables par les personnes qu'elles concernent ;

. La mise en oeuvre des traitements automatisés d'information nominatives est soumise à l'accomplissement de formalités préalables , la mémorisation des informations nominatives est encadrée par une réglementation précise et un droit général d'accès aux informations traitées est ouvert à toute personne qui pense figurer dans un fichier automatisé.

- La Commission nationale de l'informatique et des libertés (C.N.I.L.) est chargée de contrôler le respect du dispositif de protection.

Le chapitre II de la loi du 6 janvier 1978 définit la C.N.I.L. comme une institution spéciale de surveillance, autorité administrative indépendante qui est autant l'instrument de mise en oeuvre du régime de protection prévu par la loi que l'instrument d'élaboration de celle-ci (1).

Pour la mise en oeuvre de ses attributions, la Commission est dotée par la loi de très nombreuses prérogatives. C'est ainsi qu'elle détient :

. des **pouvoirs de décision** : pouvoir réglementaire pour l'élaboration de normes simplifiées ou l'édiction de règlements-type de sécurité des systèmes et faculté de prendre des décisions individuelles à l'égard des responsables de fichiers nominatifs ou des tiers mentionnés dans de tels fichiers ;

. des **pouvoirs d'avis** : avis conforme pour les informations relatives à l'origine raciale, aux opinions politiques, philosophiques ou religieuses ou aux appartenances syndicales, avis motivé pour la décision réglementaire de création des traitements du secteur public, avis simple enfin, notamment pour les décrets autorisant l'utilisation du répertoire national d'identification des personnes physiques en vue d'effectuer des traitements automatisés ;

---

(1) V. H. Maisl : La maîtrise d'une interdépendance. Commentaire de la loi du 6 janvier 1978, J.C.P. 1978 I. 2891, n° 7

. des **pouvoirs de proposition :** l'article 45 de la loi réserve à la Commission la faculté de proposer au Gouvernement de décider par décret en Conseil d'Etat l'extension de tout ou partie de la loi aux fichiers manuels et mécanographiques qui présenteraient des dangers pour les libertés ;

. des **pouvoirs de recommandation** dont la Commission a usé abondamment et régulièrement depuis son installation ;

. des **pouvoirs de contrôle** : la Commission "est chargée de veiller au respect des dispositions de la loi", tant *a priori*, par l'examen des formalités de mise en oeuvre des traitements, qu'*a posteriori*, grâce à de larges pouvoirs d'investigation complétés par des pouvoirs d'avertissement et de dénonciation des infractions au parquet ;

. enfin, des **pouvoirs d'information** qui méritent d'être signalés ici en raison de leur incidence sur la détermination des éléments constitutifs des infractions : c'est ainsi que la Commission met à la disposition du public la liste des traitements et précise pour chacun d'eux les éléments essentiels du traitement ; elle tient également à la disposition du public ses décisions, avis et recommandations dont la connaissance est utile à l'application ou à l'interprétation de la loi ; on notera toutefois que les traitements intéressant la sûreté de l'Etat, la défense ou la sécurité publique échappent à la publication.

- Un dispositif spécifique garantit la protection finale des personnes en matière de traitements automatisés d'informations nominatives.

Le champ du droit pénal en matière de protection juridique des personnes à l'égard de tels traitements est largement étendu. Il est défini par les délits correctionnels prévus par les articles 41 à 44 de la loi précitée du 6 janvier 1978, auxquels s'ajoutent les incriminations particulières destinées à sanctionner divers agissements contraires aux règles posées en matière de protection du consommateur dans le domaine de certaines opérations de crédit (article 25 de la loi du 10 janvier 1978), de centralisation de la documentation relative à la circulation routière (articles 9 et 10 de la loi du 24 juin 1970), d'automatisation du casier judiciaire (loi du 4 janvier 1980) et des listes électorales pour les élections prud'homales (articles R. 531-1 et R. 531-2 du Code du travail), de traitements d'informations statistiques nominatives par l'I.N.S.E.E...

Les incriminations ainsi créées relèvent de trois catégories d'infractions :

. infractions en matière de mise en oeuvre des traitements ;

. infractions en matière de mémorisation des informations nominatives ;

. infractions en matière de droit d'accès (1).

(1) Cette classification est retenue par plusieurs auteurs et notamment par le Professeur Raymond Gassin. (v. Informatique et libertés in Jurisclasseur pénal).

Les infractions en matière de mise en oeuvre des traitements

La loi du 6 janvier 1978 définit tout d'abord trois types d'infractions en matière de mise en oeuvre des traitements :

. Le délit de non observation des formalités administratives préalables à la mise en oeuvre des traitements automatisés d'informations nominatives qui est puni d'un emprisonnement de six mois à trois ans et d'une amende de 2 000 à 20 000 francs, ou de l'une de ces deux peines seulement (article 41).

. Le délit de détournement de finalité d'informations nominatives qui est puni d'un emprisonnement d'un an à cinq ans et d'une amende de 20 000 à 2 000 000 francs (article 44) ;

. Le délit de divulgation d'informations nominatives qui est puni d'un emprisonnement de deux à six mois et d'une amende de 2 000 à 20 000 francs, ou de l'une de ces deux peines seulement (article 43, alinéas 1er et 2).

A ces trois incriminations définies par la loi de 1978, l'article 777-3 du Code de procédure pénale introduit par la loi du 4 janvier 1980, ajoute le délit de rapprochement ou de connexion du casier judiciaire national automatisé avec un autre fichier ou recueil de données nominatives ; ce délit est puni des peines de l'article 44 de la loi de 1978, soit un emprisonnement d'un an à cinq ans et une amende de 20 000 à 2 000 000 francs, c'est-à-dire les peines les plus lourdes prévues par ce texte.

Les infractions en matière de mémorisation des informations nominatives

En matière de mémorisation d'informations nominatives, le délit principal est défini par l'article 42 de la loi précitée de 1978 qui incrimine la violation des règles d'enregistrement et de conservation des informations nominatives définies par la loi "informatique et libertés" et punit ces agissements d'une peine d'emprisonnement d'un an à cinq ans et d'une amende de 20 000 à 2 000 000 francs, ou de l'une de ces deux peines seulement.

Ces dispositions ont été adaptées aux conséquences de l'automatisation du casier judiciaire par la loi du 4 janvier 1980. Aux termes des alinéas 2, 3 et 4 du nouvel article 777-3 du Code de procédure pénale institué par l'article 6 de ce texte, toute infraction constitutive d'un délit de mention de condamnation sur un fichier quelconque est punie des peines prévues à l'article 44 de la loi précitée du 6 janvier 1978.

On rapprochera également de ces dispositions le délit d'enregistrement de l'exercice par un emprunteur de sa faculté de rétractation définie par les articles 7 et 25 de la loi du 10 janvier 1978 relative à la protection des consommateurs dans le domaine de

certaines opérations de crédit ; cette infraction est punie de 2 000 à 200 000 francs d'amende.

Les infractions en matière de droit d'accès

A la différence des infractions examinées jusqu'à présent, l'accès aux informations traitées par les personnes intéressées ne donne lieu qu'à des contraventions de police qui figurent dans le décret du 23 décembre 1981.

. La protection des logiciels par le droit d'auteur

La loi n° 85-660 du 3 juillet 1985 relative aux droits d'auteur, comporte un titre V consacré à la protection des logiciels. Introduit par le Sénat, ce dispositif a pour objet d'étendre aux logiciels la protection dont bénéficient les droits d'auteur sous réserve de son adaptation aux caractères spécifiques de l'oeuvre protégée.

Conscient des limites de la responsabilité et de la concurrence déloyale (1) et soucieux de sanctionner la contrefaçon des logiciels et de leur apporter une protection juridique adaptée, le législateur, tout d'abord peu enclin à insérer le logiciel parmi les oeuvres de l'esprit protégées par un droit d'auteur (2), a finalement introduit un mécanisme spécifique destiné à la protection des logiciels par le droit d'auteur.

La question du régime de protection juridique des logiciels a fait l'objet de nombreuses controverses ; en effet, si comme l'écrivait notre collègue Charles Jolibois, rapporteur de la commission spéciale du Sénat chargée d'examiner le projet de réforme, "la nécessité de protéger les logiciels est devenue une préoccupation aiguë dans tous les pays industriels", "le débat sur les modalités est ouvert depuis vingt ans" (3).

- Le logiciel reconnu comme oeuvre de l'esprit bénéficie de la protection accordée au droit d'auteur

Trois voies semblaient pouvoir être empruntées afin d'apporter une protection juridique aux logiciels :

---

(1) En effet, celle-ci protège l'auteur contre une appropriation, mais non contre une utilisation du logiciel ; d'autre part, son application requiert que l'appropriation soit déloyale et que l'auteur du programme rapporte la preuve de la faute, de l'acte déloyal et du préjudicie subi ; enfin, elle protège l'auteur à l'égard de ses concurrents, mais elle est inefficace à l'égard de non-concurrents.

(2) V. JO. A.N. Débats, 29 juin 1984, p. 3905.

(3) Sénat n° 212 (1984-1985), T. I. p. 54.

- la protection par brevet ;

- le recours au droit d'auteur ;

- une législation *sui generis*.

. L'inadaptation de la protection par brevet

La commission spéciale du Sénat a tout d'abord constaté que, dans son article 6, la loi du 2 janvier 1968 modifiée excluait expressément les programmes d'ordinateurs du champ d'application du **droit des brevets.**

Cette **exclusion légale** dont la portée a toutefois été **tempérée par la jurisprudence** qui admet qu'un logiciel peut bénéficier de la protection de la loi en tant qu'élément d'un procédé industriel lui-même brevetable (1), est **loin de suffire à assurer une protection suffisante,** d'autant que les logiciels remplissent difficilement les conditions imposées par la législation relative aux brevets, soit les caractères de nouveauté, d'activité inventive et, surtout, d'application industrielle.

Le coût élevé de la procédure du dépôt de brevet et la complexité du régime de la protection internationale des brevets ont conduit à écarter, sans plus hésiter, cette solution mal adaptée aux objectifs poursuivis.

. L'échec des tentatives pour créer un droit *sui generis*

La solution d'un droit *sui generis* a également été écartée en raison de **l'échec des tentatives** de rédiger une législation-type engagées par certaines organisations internationales telles que **"l'Organisation mondiale de la propriété industrielle** (OMPI).

Les réflexions conduites par bon nombre de pays industrialisés se sont rapidement détournées de la voie ainsi ouverte, afin de privilégier des solutions susceptibles de s'inscrire dans le droit en vigueur, tant national qu'international.

. L'accueil par le droit d'auteur

Un examen attentif du droit d'auteur et de la jurisprudence (2) à laquelle son application aux logiciels avait déjà donné lieu, a conduit la commission spéciale du Sénat à juger que cette forme de protection juridique pouvait être considérée comme le **moyen le plus souple et le mieux adapté** à l'objectif poursuivi ; toutefois, constatant que la législation relative au droit d'auteur devait subir certains aménage-

---

(1) Cour d'appel de Paris, 15 juin 1981, société Schlumberger.

(2) voir notamment TGI Paris, 21 septembre 1983 Affaire Apple Computer : "l'effort personnel du créateur est déterminant dans le résultat obtenu, l'évidence commande de retenir le caractère d'oeuvre de l'esprit aux programmes d'ordinateurs."

ments destinés à prendre en compte les caractères spécifiques des logiciels, la commission a proposé "de prévoir expressément que la loi du 11 mars 1957 s'applique aux logiciels **avec toutefois des adaptations tenant compte des problèmes particuliers qui se posent dans ce domaine**" (1)

En conséquence, la loi précitée du 3 juillet 1985 pose tout d'abord **comme principe fondamental que les logiciels sont** considérés comme **des oeuvres de l'esprit protégées** : c'est à ce titre qu'ils sont insérés dans la longue liste de l'article 3 de la loi précitée de 1957. Dans un second temps, la loi consacre son **titre V** à **des dispositions spécifiques de protection** des logiciels (articles 45 à 51).

- Les logiciels sont protégés par des prérogatives adaptées du droit d'auteur

Le titre V de la loi précitée du 3 juillet 1985 apporte des aménagements à la loi du 11 mars 1957 en tant que celle-ci s'applique aux logiciels :

. L'employeur est le titulaire du droit d'auteur sur les logiciels élaborés par ses salariés ;

. Le droit de l'auteur est limité ;

. Les auteurs bénéficient d'une protection renforcée contre la copie et l'utilisation non autorisée de logiciels :

La loi de 1957 ne protège pas les droits des auteurs contre les copies réservées à un usage privé ni surtout contre l'utilisation non autorisée de logiciels. L'article 47 de la loi du 3 juillet 1985 introduit sur ce point une dérogation au droit commun de la protection des droits d'auteur en disposant que, sous réserve d'une copie de sauvegarde, **toute reproduction ainsi que toute utilisation d'un logiciel réalisées sans le consentement exprès de l'auteur sont constitutives de délits de contrefaçon et sont, de ce fait, punies** des peines prévues aux articles 425 à 429 du code pénal, soit une peine d'emprisonnement de trois mois à deux ans et une amende dont le montant est fixé entre 6 000 et 120 000 F ou seulement l'une de ces deux peines ; en outre, le tribunal pourra prononcer la confiscation de tout ou partie des recettes procurées par l'infraction ainsi que des exemplaires reproduisant illicitement le logiciel.

. La durée de protection des droits d'auteur des logiciels est réduite à vingt-cinq ans ;

. La rémunération de la cession d'un logiciel peut être évaluée forfaitairement ;

. Les modalités d'exécution de la saisie-contrefaçon sont adaptées aux caractères propres des logiciels ;

---

(1) Rapport précité, p. 67.

. Les créateurs étrangers jouissent des droits attachés à la protection des logiciels ;

L'article 51 de la loi du 3 juillet 1985 accorde aux **créateurs étrangers la même protection** qu'aux créateurs français, **sous réserve** que leur Etat réponde à la **condition de réciprocité.** On notera, à cet égard, que de nombreux Etats ont ratifié la convention de Berne : dès lors, **les créations françaises peuvent obtenir une protection juridique auprès des tribunaux étrangers.**

Les deux dispositifs ainsi examinés ne sont que les chapitres répressifs de lois spéciales et ne sauraient en tout état de cause constituer la législation de portée générale dont la nécessité se fait sentir.

C. L'apparition progressive d'une législation spécifique à portée générale : l'exemple américain

L'exemple le plus intéressant d'une législation informatique pénale est apporté par les Etats-Unis dont la pratique en la matière est déjà ancienne.

En 1984, une loi fédérale intitulée "counterfeit access device and computer fraud abuse act" est venue sanctionner les délits informatiques. Par ailleurs, un certain nombre d'incriminations pénales ont été étendues à l'informatique : la contrefaçon, l'escroquerie réalisée au moyen de l'utilisation du système postal et des systèmes de télécommunications, le transport et le recel de biens volés, l'association de malfaiteurs, le "racket" et l'utilisation frauduleuse de cartes de crédit.

Sous l'impulsion du sénateur Abraham Ribicoff, le droit fédéral a donc largement assimilé les délits informatiques que certains Etats américains, notamment la Californie, avaient déjà inscrits dans leur arsenal répressif.

. *Les différents dispositifs existant aux Etats-Unis répriment un ensemble non négligeable d'agissements frauduleux*

La législation des Etats américains se présente comme une réponse aux différents délits informatiques constatés à ce jour. A cette fin, elle définit un ensemble de comportements délictueux :

- **l'accès non autorisé** à un système ("trespassing") ;

- **le vol** ("theft"), qu'il s'agisse d'un détournement de fonds, d'un vol de services assimilable à un vol d'usage, d'un vol de logiciel, du vol ou de la détérioration d'une donnée ; on remarquera que **l'information**

est assimilée, en droit américain, **à une "property"**, elle est donc considérée comme un bien ;

- **le sabotage** ("malicious destruction"), soit des logiciels, soit des données (effacement) ;

- **les utilisations frauduleuses** de l'informatique dans le dessein d'obtenir une somme indue, une information protégée... ; il s'agit alors de **l'extension pure et simple d'incriminations préexistantes** (violation de la vie privée, destruction de composants informatiques...).

. La notion de propriété a du être redéfinie

Le droit anglo-saxon retient sous le vocable générique de **"property", une définition** particulière de la propriété, **susceptible d'être appliquée à des biens immatériels** ("intangible items") ; cependant, il s'est avéré que le vol d'une information enregistrée dans un système de traitements automatisés de données échappait à la sanction lorsque le support matériel de la donnée n'avait pas été soustrait. En conséquence, les Etats ont adopté une définition plus extensive de la notion de "property", afin d'englober les données ou les instructions contenues dans les systèmes informatiques.

C'est ainsi que l'Alaska a retenu une définition particulièrement large qui considère comme "property" tout "élément, contenu ou objet de valeur, y compris l'argent, les propriétés personnelles corporelles ou incorporelles, y compris les données, ou les informations stockées dans un logiciel, un système, un réseau..." (1).

D'une façon générale, la législation se réfère à **trois catégories de biens informatiques** : **le "hardware"**, c'est-à-dire les biens corporels comme les machines, y compris les composants électroniques, **le "software"**, c'est-à-dire les éléments incorporels liés à la programmation (logiciels, données en mémoire et procédures de traitements) -dans certains cas comme la Californie, les instruments financiers sont également compris sous cette rubrique- et, enfin, **les services**, c'est-à-dire la capacité de traitement du système.

---

(1) "Article, substance, or thing of value, including money, tangible or intangible personal property, including data or information, stored in a computer program, system or network...".

. L'échelle des peines a été aggravée

Selon les Etats, l'échelle des peines est éminemment variable, depuis les peines contraventionnelles californiennes **jusqu'aux peines criminelles** (10 ans de prison) prévues par la législation de l'Oklahoma.

L'échelle varie essentiellement en fonction de la qualification des délits ("misdemeanor" dans les Etats peu répressifs et "felony" dans les Etats plus répressifs) et du type de dommages occasionnés. Des **circonstances aggravantes** viennent alourdir les peines en raison de **la qualité de la victime** (service public ou système administratif par exemple) ou de **la nature particulière du délit** (espionnage ou trahison), tandis que sous certaines conditions, le montant de l'amende reste proportionnel à **la valeur de la propriété** violée ou détruite ou encore à **l'importance du résultat** obtenu.

. La législation fédérale garantit une meilleure efficacité de la répression

Depuis l'adoption, en **1984**, de la première loi fédérale sur le "computer crime" et, en **1986**, du "computer fraud and abuse act", la législation fédérale dispose d'incriminations fédérales spécifiques.

En vertu de ces textes, sont considérés comme des délits informatiques :

- le fait d'obtenir, en connaissance de cause, ("knowingly") des informations que le Gouvernement américain considère comme secrètes en raison des nécessités de la défense nationale et des relations extérieures ;

- le fait d'accéder intentionnellement ("intentionally") aux bases de données des établissements financiers ou des établissements de crédit (notamment de crédit à la consommation) ;

- le fait d'accéder intentionnellement et sans autorisation à un ordinateur alors que celui-ci est réservé à l'usage exclusif du Gouvernement des Etats-Unis ou qu'il est utilisé par ou au bénéfice du Gouvernement et que cet accès affecte cet usage ;

- le fait, en connaissance de cause et dans une intention frauduleuse ("intent to defraud"), d'accéder, sans autorisation, à un ordinateur d'intérêt fédéral, d'excéder l'autorisation d'accès accordée pour un tel ordinateur et par ce moyen de se livrer à des agissements frauduleux destinés à obtenir quelque chose de valeur, à l'exception des cas où le bénéfice de la fraude se limite à l'utilisation de l'ordinateur ;

- le fait, en connaissance de cause, d'accéder sans autorisation à un ordinateur d'intérêt fédéral et, soit d'altérer les informations contenues dans la machine, soit d'empêcher l'utilisation normale de l'ordinateur, le préjudice ainsi causé étant supérieur à 1 000 dollars sur une année ;

- enfin, le fait, en connaissance de cause et dans une intention frauduleuse, de faire usage de mots de passe secrets ou de toute autre information susceptible de permettre l'accès sans y avoir été autorisé.

On notera par ailleurs qu'à ces six incriminations, le "credit card fraud act" de 1984 ajoute la contrefaçon des cartes de crédit permettant l'accès aux systèmes de traitements automatisés, l'utilisation de telles cartes et la détention du matériel de contrefaçon.

. La législation fédérale comporte des définitions précises

La nouvelle section 1030 du titre 18 du code fédéral définit deux notions fondamentales inhérentes au dispositif répressif :

- **le "computer"** qui inclut tous les procédés électroniques, magnétiques, optiques, électromécaniques ou autres, destinés au traitement à grande vitesse des données (1) ; cette définition comprend le stockage des données et les systèmes de communications directement reliés à l'ordinateur ;

- **l'expression "exceeds authorized access"**, qui concerne ceux qui étant habilités à accéder à un système ont utilisé cette autorisation pour obtenir ou modifier des informations qu'ils n'avaient pas de titre à obtenir ou à modifier.

On relèvera également que ce dispositif opère une distinction entre "knowing" (en connaissance de cause), "intentional" (intentionnel) (2) et "with intent to defraud" (dans l'intention de commettre un délit), de même qu'il distingue clairement entre les accès autorisés et les accès non autorisés.

. La gravité des peines prévues par la législation fédérale

La loi de 1986 punit les délits portant sur des données classifiées d'une peine de prison pouvant atteindre dix ans ; de tels agissements sont en effet considérés comme des crimes fédéraux. En cas de piratage des banques de données ou des systèmes de traitements des établissements financiers ou de crédit, les peines encourues montent à **vingt ans de prison**.

Les accès non autorisés et l'utilisation abusive des codes et des mots de passe sont punissables d'un an de prison et d'une amende, ou de l'une de ces deux peines seulement.

---

(1) "Electronic, magnetic, optical, electromechanical or other high-speed data processing device(s)".

(2) Le rapport parlementaire considère qu'il y a une différence de degré entre la connaissance de cause et l'intentionnel : "a slight higher state of mine standard".

Enfin, les piratages comportant une modification des données ou empêchant l'utilisation normale du système sont punissables de cinq ans de prison et d'une amende, ou de l'une de ces deux peines seulement.

D. Législation spécifique ou extension de délits préexistants ?

L'examen des modifications récemment introduites dans les législations pénales des pays industriels montre que d'une façon générale, ils se contentent, pour l'instant, d'élargir certaines incriminations préexistantes à l'informatique, plutôt que de définir un droit nouveau.

. Le "pis aller" de l'extension d'incriminations préexistantes

En privilégiant une **approche** de la fraude informatique, **par le résultat frauduleux** auquel celle-ci permet d'aboutir, un certain nombre d'Etats ont inclu les délits informatiques dans leur système pénal.

A ce titre, quatre domaines ont fait l'objet d'attentions toutes particulières :

- le **faux informatique** : le Royaume-Uni (1981), l'Australie (1983), l'Autriche (1985), la Suisse (1985) et l'Allemagne (1986) incriminent le faux fabriqué au moyen de falsifications ou de modifications apportées à des données informatisées ou introduites dans des traitements automatisés ; ils incriminent également l'usage de tels faux ;

- **l'escroquerie** : le gain indu obtenu au moyen d'une action sur les systèmes informatiques est spécifiquement incriminé par les législations australienne (1985), autrichienne (1985), danoise (1985), suédoise (1985), suisse (1985) et allemande (1986) ;

- **l'abus de confiance et la divulgation de procédés** en relation avec l'informatique sont incriminés en tant que tels en Suisse (1986) et en Allemagne (1986) ;

- **l'espionnage informatique** incriminé en Allemagne depuis 1986 (1).

---

(1) La législation allemande comporte de nombreuses dispositions relatives aux fraudes informatiques ; toutefois, l'optique retenue est particulière, dans la mesure où ce droit fait partie intégrante du domaine des "crimes économiques".

. L'apparition timide de délits informatiques

Certaines législations incriminent des délits informatiques *stricto sensu*, quels que soient les résultats obtenus.

A ce jour, trois domaines ont été explorés :

-**l'accès frauduleux** à un système de traitements automatisés de données, réprimé au Danemark (1985) et en Norvège ;

- **l'utilisation frauduleuse des capacités de traitement** d'un système, incriminée au Canada et en Suisse (1985) ;

- **la modification ou la destruction des données ou des logiciels,** visées par les législations danoise ("empêche le fonctionnement normal"), allemande (sabotage logique), autrichienne, norvégienne et suisse.

L'examen de la proposition de loi auquel nous allons maintenant procéder, nous permettra de constater que l'Assemblée nationale a souhaité privilégier cette voie de la définition d'incriminations spécifiques, sans toutefois respecter parfaitement -nous semble-t-il- la ligne qu'elle s'était ainsi fixée à elle-même.

TROISIEME PARTIE

LES TRAVAUX DE L'ASSEMBLEE NATIONALE

Le 15 juin 1987, l'Assemblée nationale a adopté la proposition de loi qui vous est aujourd'hui soumise, dans une rédaction sensiblement différente de celle qui avait été proposée par son auteur initial, M. Jacques Godfrain.

A. La proposition Godfrain : une démarche avant tout pragmatique

Afin de "trancher les hésitations jurisprudentielles et les querelles doctrinales" (1), M. Godfrain a choisi de "retoucher" un certain nombre d'articles du code pénal ; par ce moyen, il s'est efforcé d'étendre le champ d'incriminations préexistentes pour y ranger expressément des procédés frauduleux associés à certaines utilisations de l'informatique.

Cette démarche ne lui permettant pas d'incriminer certains agissements frauduleux pourtant constatés dans la pratique, il a également proposé de définir de nouveaux délits.

. Le choix de l'extension de certaines incriminations préexistantes

La démarche adoptée par M. Godfrain s'apparente à celle que certaines législations étrangères ont suivie ; ainsi en est-il, par exemple, de l'Allemagne qui a renforcé son droit pénal économique en classant les manipulations informatiques au nombre des moyens de commettre des délits déjà définis par des textes répressifs préexistants.

La proposition de loi initiale procède de la même manière pour toute une série d'infractions :

- **le faux en écriture informatique** : l'enregistrement informatique expressément qualifié d'"écriture" ou de "document" au sens du code pénal, devient susceptible de faire l'objet de falsifications (article premier) ;

---

(1) Proposition A.N. n° 352 (huitième législature), 5 août 1986, p. 3.

- **l'usage du faux informatique** comme élément constitutif d'une escroquerie : l'utilisation indue d'un code d'accès ou d'identification est définie comme une manoeuvre frauduleuse (art. 5) ;

- le fait de se faire délivrer, au moyen de l'une des manoeuvres frauduleuses visées par l'article 405 du code pénal, des données ou programmes enregistrés, est qualifié **d'escroquerie** (art. 5) ;

- **l'abus de confiance** en cas de divulgation ou de détournement des données ou programmes enregistrés, prêtés ou loués dans les conditions prévues à l'article 408 du code pénal (art. 6) ;

- **la détérioration et la destruction volontaires des biens incorporels que sont les données et les programmes** sont punies des peines de l'article 434 du code pénal (art. 7) ;

- **la détérioration et la destruction** d'enregistrements informatiques contenant ou opérant obligation, disposition ou décharge, ou d'enregistrements contenant des éléments susceptibles de faciliter la recherche des crimes et délits : ces agissements sont punis des peines **aggravées** de l'article 439 du code pénal (art. 8).

. *"L'enregistrement informatique" : une notion imprécise*

La notion centrale d'enregistrement informatique autour de laquelle est construite la définition du faux informatique n'est pas sans soulever des incertitudes quant à son contenu et à sa portée.

En effet, **l'assimilation des enregistrements informatiques à des écrits** paraît pour le moins hasardeuse, si l'on considère l'absence de stabilité de ces enregistrements auxquels le droit ne reconnaît d'ailleurs pas valeur de preuve (1).

L'informatique a pour conséquence de supprimer le support-papier, ce qui rend difficile l'administration traditionnelle d'une preuve par la présentation d'un document écrit et signé.

La loi du 12 juillet 1980, initiée par une proposition de loi que j'avais eu l'honneur de déposer devant le Sénat, n'a pas consacré la preuve apportée par la bande magnétique qui était pourtant l'un des objets de cette proposition. L'article 1348 du code civil, dans la nouvelle rédaction introduite par cette loi, a en revanche reconnu l'intérêt de procédés reprographiques sûrs à propos desquels il admet le remplacement de l'écrit par une copie fidèle et durable. Au sens de cet article, est réputée durable toute reproduction indélébile de l'original, toute modification du support étant irréversible ; or **l'enregistrement informatique** diffère substantiellement de l'écrit en tant qu'il **peut,** contrairement au support-papier, **être aisément modifié,** qu'il n'est pas signé à proprement dire et, enfin, que la distinction entre copie et original est dépourvue de signification.

---

(1) Si ce n'est en matière commerciale où la preuve peut se faire par tout moyen.

Certes, le développement de nouvelles techniques comme la digitalisation d'un écrit et la mise au point d'un procédé tel que le résultat de la reconstitution de l'original puisse être tenu pour fidèle et durable, sont les prémisses annonciateurs d'une possible évolution dans les années à venir ; toutefois, en l'état actuel des techniques d'enregistrement, il semble peu réaliste et surtout dangereux de vouloir assimiler l'enregistrement informatique à un écrit.

On soulignera **toutefois** que les documents informatiques peuvent constituer **des compléments de preuve,** susceptibles de compléter des commencements de preuve par écrit ; ils peuvent même constituer **des commencements de preuve** par écrit, sous la triple condition fixée par l'article 1347 du code civil, qu'ils se présentent sur un support qui les rendent directement intelligibles, qu'ils aient été créés antérieurement à la contestation et qu'ils émanent de la partie contre laquelle ils sont allégués.

Il apparaît, en conséquence, que la démarche suivie par M. Godfrain est encore prématurée, car qu'il s'agisse des pays de "common law" ou de ceux qui, comme la France, connaissent le régime de la preuve légale, tous les systèmes juridiques restent aujourd'hui aux prises avec la nécessité d'élaborer de nouvelles règles pour établir la preuve en matière informatique et cette difficulté n'est pas sans incidence sur les risques potentiels soulevés par la rédaction proposée pour l'article 165 du code pénal.

. La définition de nouvelles incriminations

Outre l'extension d'incriminations préexistantes, la proposition de loi initiale définit deux incriminations nouvelles :

- **"l'entrée sans droit" ou la "tentative d'entrée sans droit" dans tout ou partie d'un système de traitement de l'information** (art. 2 et 3) ;

- **la captation sans droit de données ou programmes enregistrés** : cette incrimination s'analyse en fait en une transposition des dispositions relatives au vol (art. 4).

Ces deux dispositions sont en fait destinées à ranger les systèmes informatiques, les données et les programmes au nombre des biens susceptibles d'être volés, tandis que notre droit les exclut de la protection pénale prévue à l'article 379 du code pénal.

Ce souci d'assurer une protection des systèmes informatiques contre les intrusions dont ils peuvent faire l'objet, constitue l'un des aspects les plus intéressants du dispositif proposé par M. Godfrain, dans la mesure où il se détache des conséquences -par exemple en termes de gains financiers illicites- qui peuvent résulter de ces intrusions non autorisées.

Soucieuse de garantir la protection des systèmes informatiques eux-mêmes contre toute atteinte extérieure, l'Assemblée nationale s'est

principalement attachée à retenir cet aspect du texte initialement proposé.

B. Les travaux de l'Assemblée nationale : protection des systèmes et préservation de l'authenticité des données

Le texte adopté par l'Assemblée nationale prévoit l'introduction par un chapitre nouveau inséré dans le code pénal, de deux catégories de dispositions :

- la première sanctionne **"l'accès frauduleux"** à un système de traitement automatisé de données (art. 462-2, premier alinéa) ;

- les secondes ont pour objet de protéger ces systèmes contre **les atteintes portées à leur bon fonctionnement** (art. 462-2, second alinéa, et art. 462-3 pour le sabotage) **ou à l'authenticité des données** qui y figurent (art. 462-4, premier alinéa, pour la détérioration ou la destruction ; art. 462-4, second alinéa, et 462-5 pour la falsification des données et l'usage de données falsifiées).

Le dispositif ainsi élaboré est convaincant ; il appelle toutefois quelques remarques et certaines réserves.

. Une définition extensive du "système de traitement automatisé de données"

M. René André, rapporteur de la proposition de loi à l'Assemblée nationale, a suggéré d'évoquer les "systèmes de traitements automatisés de données", ce qui constitue une innovation importante par rapport à la notion d'informatique traditionnellement rattachée à une conception déjà ancienne de l'ordinateur envisagé comme une machine autonome et isolée, fonctionnant en circuit fermé.

Le rapporteur a tout d'abord souligné que cette notion s'inspirait, sur le plan terminologique, de **la loi du 6 janvier 1978** relative à l'informatique, aux fichiers et aux libertés qui **emploie l'expression voisine de "traitement automatisé d'informations nominatives" qu'elle définit** comme "tout ensemble d'opérations réalisées par des moyens automatiques, relatif à la collecte, l'enregistrement, l'élaboration, la modification, la conservation, la destruction d'informations nominatives ainsi que tout ensemble d'opérations de même nature se rapportant à l'exploitation de fichiers ou bases de données et notamment les interconnexions ou rapprochements, consultations ou communications d'informations nominatives" (1).

---

(1) Art. 5 de la loi n° 78-17 du 6 janvier 1978 (JO du 7 janvier 1978).

A l'occasion de la définition du champ d'application de la nouvelle incrimination d'"accès frauduleux, direct ou indirect", le rapporteur a indiqué qu'il distinguait en fait entre les systèmes, eux-mêmes composés des "mémoires vives, mémoires de masse : disquettes, bandes...", et les moyens d'accès à ces systèmes constitués par les terminaux d'accès à distance, les réseaux assurant la communication entre les divers éléments d'un système ou encore entre plusieurs systèmes (1). Si ce **souci de définition** mérite d'être souligné, on regrettera toutefois qu'une **distinction** soit ainsi opérée **entre les systèmes,** conçus comme des capacités de stockage et de traitement, **et les accès à ces systèmes** qui sont, en fait, des parties intégrantes de ces systèmes ; on regrettera également qu'**aucune définition du système ne figure dans le texte lui-même.**

. *Une légère incertitude sur les éléments constitutifs de l'infraction d'accès frauduleux*

Le premier alinéa de l'article 462-2 du texte est relatif à **l'accès frauduleux à un système de traitement automatisé de données : c'est l'incrimination fondamentale du texte** et il n'y a pas lieu de la remettre en question.

On notera toutefois que, dans sa rédaction actuelle, cette disposition est applicable à toutes les intrusions dans un système, sous réserve de l'appréciation souveraine que le juge portera sur le caractère frauduleux de l'accès. Le rapporteur a précisé qu'il convenait de considérer qu'"il y aura accès frauduleux dès lors qu'on cherchera à s'introduire indûment dans un système protégé par un dispositif de sécurité" (2) et le Garde des Sceaux a souligné au cours des débats que "le droit pénal ne doit pas compenser l'insuffisance ou la défaillance des mesures de sécurité" (3). Cette **exigence d'une protection du système** pour que l'infraction soit constituée paraît raisonnable ; on regrettera, là encore, qu'elle ne soit **pas explicitement inscrite dans la loi.**

. *Le sabotage exige-t-il la création d'une incrimination spécifique ?*

Le texte adopté par l'Assemblée nationale distingue entre deux catégories de dommages causés aux systèmes de traitements automatisés de données :

---

(1) V. rapport A.N. n° 744 (huitième législature), 14 mai 1987, p. 13.

(2) V. rapport précité, p. 13.

(3) V. JO Débats A.N. 16 juin 1987, p. 2386

- les dommages involontaires causés à l'occasion d'un accès frauduleux au système (art. 462-2, deuxième alinéa) ;

- les dommages volontaires assimilables à un sabotage soit matériel, soit fonctionnel du système (art. 462-3).

S'il paraît nécessaire de prévoir, en tant que telles, les conséquences dommageables d'une intrusion frauduleuse et d'y associer une aggravation des peines encourues en cas de simple accès frauduleux sans dommage pour le système, il est en revanche plus douteux qu'il faille spécifiquement incriminer le sabotage, c'est-à-dire les agissements dont l'unique objet est d'endommager le système ; en effet, il apparaît que **de tels agissements sont susceptibles d'entrer dans la catégorie plus générique de piratage** dont ils sont une forme possible.

D'autre part, en dépit des assurances fournies par le rapporteur qui se fondait pour cela sur une décision du Conseil constitutionnel (1), il est à craindre que dans l'éventualité d'un conflit du travail, une équivoque ne soit créée par l'emploi du terme "entrave"..

. Les risques d'une réintroduction du faux informatique

La rédaction initiale de M. Godfrain proposait de réputer comme écriture ou document tout enregistrement informatique (article premier) et permettait, par voie de conséquence, de réprimer le faux informatique.

Le rapporteur de l'Assemblée nationale, après avoir exprimé les plus expresses réserves sur une telle approche qu'il a qualifié à la fois d'imprécise (2) et d'inadéquate (3), a ensuite **proposé de sanctionner les atteintes portées à l'authenticité des données, en incriminant, d'une part, les manoeuvres conduisant à "une altération de la vérité" (art. 462-4, second alinéa) -on retrouve là le faux informatique- et, d'autre part, l'usage de documents reproduisant des informations ainsi altérées (art. 462-5) -il s'agit incontestablement de l'usage de faux informatique.** On s'étonnera d'une telle rédaction alors que les réserves émises par M. André semblaient pourtant parfaitement fondées.

---

(1) V. JO Débats A.N., 16 juin 1987, p. 2388

(2) V. rapport précité p. 9.

(3) V. rapport précité p. 10.

. La confiscation des matériels : une menace qui peut être efficace

Sur un amendement de M. Godfrain, l'Assemblée nationale a également adopté un article 462-6 destiné à donner au juge la faculté d'ordonner la confiscation des matériels ayant servi à commettre l'une des infractions ainsi définies.

Cette disposition, conçue comme "un moyen de freiner la fraude informatique" (1), peut en effet jouer **un rôle préventif** efficace, notamment à l'égard de jeunes délinquants sensibles à la menace de la perte de leur matériel informatique.

Le texte issu des travaux de l'Assemblée nationale constitue une approche très remarquable du phénomène de la fraude informatique et **le choix d'un dispositif répressif spécifiquement applicable à cette nouvelle forme de délinquance doit être retenu, sous réserve des quelques modifications ou précisions que votre commission vous proposera d'introduire.**

(1) Intervention de M. Godfrain, JO Débats A.N. du 16 juin 1987, p. 2388.

QUATRIEME PARTIE

LES PROPOSITIONS DE LA COMMISSION

Votre commission des Lois souscrit sans réserve à la ligne de conduite fixée par l'Assemblée nationale qui "vise à protéger le système informatique lui-même contre toute atteinte de l'extérieur" (1) ; elle vous propose toutefois d'introduire une définition du système de traitements automatisés de données et du maître du système, de retenir l'incrimination générale de piratage informatique et enfin de renoncer à une protection de l'authenticité des données dont la parenté avec la notion de faux informatique soulève plus de difficultés qu'elle n'en résoud.

A. La nécessité de donner des définitions précises

Il est rare qu'un texte pénal français soit précédé par des définitions qui en éclairent la portée, alors que cet usage est constant à l'étranger. Ce constat peut s'expliquer par deux considérations souvent convergentes : d'une part, il n'est pas de bonne politique législative que ce soit par le biais d'un texte répressif que des définitions fassent leur apparition dans le champ juridique, d'autre part, les dispositions répressives se réfèrent généralement à des définitions préexistantes apportées par le droit civil ou commercial.

On pourrait, en conséquence, se résoudre à s'en remettre à un -hypothétique- futur "code de l'informatique" pour apporter les définitions nécessaires, préférer s'en tenir à proposer quelques approches à l'occasion des travaux parlementaires dont on sait qu'ils sont peu consultés, ou encore, et c'est là le raisonnement suivi par l'Assemblée nationale, choisir de confier au juge répressif la tâche délicate de progressivement et lentement définir l'exacte portée de la loi.

Aucune de ces solutions ne lui ayant semblé satisfaisante, votre commission a préféré se livrer au difficile exercice de la définition du système de traitements automatisés de données et du maître du système. Dans la mesure où il est impossible en une telle matière de procéder par assimilations, ces deux définitions, l'une descriptive et l'autre fonctionnelle, s'attacheront à dégager une qualification spécifique, applicable au piratage informatique.

---

(1) Rapport précité, p. 12.

. La définition du "système de traitements automatisés de données"

Le rapporteur de la commission des Lois de l'Assemblée nationale a joint en annexe de son rapport des éléments de terminologie qui contiennent la définition des mots "informations", "données" et "logiciels" et à laquelle il convient de se référer. Il a également fort opportunément rappelé que la définition du "traitement automatisé d'informations" figure à l'article 5 de la loi du 6 janvier 1978.

En revanche, s'il a fourni des explications sur la notion de "système de traitement de données" (1), celles-ci paraissent incomplètes aux yeux de votre commission.

En effet, **un système est une organisation polymorphe et souvent transfrontière qui n'a pas la consistance d'un bien au sens habituel du terme.** Il ne saurait être question d'énoncer en une liste exhaustive les élements qui peuvent le composer et qui sont parcourus par le fluide qu'est l'information. Doivent seulement être retenus ceux de ses éléments qui en constituent les caractéristiques essentielles et dont il est vraisemblable qu'ils subsisteront dans l'évolution actuellement prévisible de l'informatique.

Encore faut-il se garder de pousser trop loin l'analyse. Pierre Nicole écrivait en 1862 dans La logique ou l'art de penser : "il serait impossible de définir tous les mots car pour définir un mot, on a nécessairement besoin d'autres mots, et si on voulait encore définir les mots dont on se serait servi pour l'explication de celui-là, on en aurait encore besoin d'autres. Il faut donc s'arrêter à des termes primitifs que l'on ne définisse point".

Ces "termes primitifs" ont, dans un texte de la nature de celui dont nous discutons, **une obligatoire connotation technologique** et il est plus simple de les employer tels quels que d'user de périphrases pour les rapprocher du langage commun.

Dans la définition qui suivra nous nous efforçons d'utiliser des mots qui ont un sens générique. Ainsi, le mot "mémoire" désignera-t-il aussi bien les mémoires vives que les mémoires mortes, les mémoires de masse, les mémoires annexes et ceci quelque soit leur support. Nous ne prendrons pas parti sur la nature de ces mémoires ce qui impliquerait des développements sur le présent et le futur, dépassant le cadre de la présente discussion.

---

(1) V. p. 47 du présent rapport

Dans cet esprit, votre commission vous propose la **définition** suivante qui doit être entendue au sens strict de l'application de la loi pénale, sans qu'il soit question d'empiéter sur les prérogatives de la commission de terminologie de l'informatique :

"Au sens du présent chapitre, on doit entendre par système de traitements automatisés de données, tout ensemble composé d'une ou plusieurs unités de traitement, de mémoires, de logiciels, d'organes d'entrées-sorties, et de liaisons, qui concourent à un résultat déterminé, cet ensemble étant protégé par des dispositifs de sécurité" **(art. 462-2-A, amendement n° 2, premier alinéa).**

Cette définition couvre la situation la plus simple, l'ordinateur isolé, et la plus complexe, le réseau aux multiples ramifications qui fait le tour de la terre.

Les organes d'entrées-sorties comprennent aussi bien le clavier, le lecteur optique, le micro, le terminal, l'imprimante, le synthétiseur ou l'outil, sans qu'il soit possible d'énumérer toutes les formes que peuvent prendre ces organes. Se trouvent également compris dans cette catégorie, les badges et les cartes magnétiques qui constituent autant d'accès au système.

Enfin, les **liaisons** font explicitement partie du système et ce point n'est pas négligeable quand on sait que de nombreuses fraudes sont perpétrées au moyen de branchements non autorisées sur les liaisons des réseaux, c'est-à-dire souvent sur les lignes de télécommunications elles-mêmes ; ces branchements pirates permettent aux délinquants soit de prendre connaissance des codes d'accès secrets des utilisateurs autorisés, soit de pénétrer directement dans les systèmes eux-mêmes (1). Le matériel destiné à capter les signaux émis sur les lignes de télécommunications est actuellement en vente libre et il suffit de brancher l'un de ces appareils sur une ligne pour pouvoir décoder et stocker les signaux transmis.

Il est également possible de prélever les informations contenues dans les rayonnements émis par les systèmes de télétraitement ; de même qu'il est aussi relativement simple de prélever des signaux échangés par faisceaux hertziens et des communications par satellites au moyen d'une antenne bien située et d'un récepteur permettant de "démoduler" l'information.

Actuellement, **l'article 368 du code pénal** incrimine l'écoute, l'enregistrement ou la transmission de paroles prononcées dans un lieu privé, sans le consentement des personnes concernées. Cette disposition introduite par l'article 23 de la loi n° 70-643 du 17 juillet 1970 tendant à renforcer la garantie des droits individuels des citoyens, punit ces agissements d'un emprisonnement de deux mois à un an et d'une

---

(1) V. par exemple les rapports de Sécuricom, congrès mondial annuel de la protection et de la sécurité informatique et des communications.

amende de 2 000 à 60 000 francs, ou de l'une de ses deux peines seulement ; elle est toutefois impuissante à réprimer des atteintes de même nature à la discrétion des communications commerciales et la liste (1) des appareils conçus pour réaliser ces infractions n'a jamais été dressée, ce qui limite d'autant l'efficacité de ce dispositif.

Il apparaît, en conséquence, qu'**il convient,** pour une répression efficace des fraudes informatiques, **d'incriminer également les accès indus aux liaisons des systèmes de traitements automatisés de données** et c'est ce qui vous est proposé par l'adjonction du terme "liaisons" dans la définition du système. Le futur texte de loi sur les télécommunications qui est encore à l'état d'avant-projet devrait d'ailleurs permettre de compléter le dispositif de protection de l'ensemble des réseaux de télécommunications, dans un contexte mieux adapté à ce problème.

Dans la mesure où le champ de la définition ainsi retenue excède la notion courante d'informatique, votre commission vous propose de **modifier l'intitulé du chapitre** que l'Assemblée nationale a introduit dans le code pénal (**amendement n°1**), et par voie de conséquence de modifier **le titre du texte lui-même (amendement n° 10) pour parler de "systèmes de traitements automatisés de données".**

. La notion de "maître du système"

On peut être "propriétaire" d'un ou plusieurs ordinateurs, de leurs liaisons à l'intérieur de l'entreprise, et des appareils les plus divers qui constituent leurs périphériques ; il est en revanche impossible d'adapter la notion de propriété à l'organisation beaucoup plus complexe des systèmes. A des installations privatives, s'ajouteront en effet des centres serveurs assurant des prestations à de nombreux bénéficiaires, ainsi que des réseaux locaux, nationaux ou internationaux dépendant de la puissance publique ou d'organismes privés. Quant aux données, nous avons vu qu'en l'absence d'un statut de l'information qui reste à élaborer, elles n'ont pas la nature d'un bien.

Dans un cadre aussi original, il vous sera suggéré de parler de "maître du système" pour désigner celui qui dispose légitimement de ce système. La notion de "maîtrise" est d'ailleurs familière au droit français, ainsi qu'en témoigne la persistance des termes "maître d'oeuvre" et "maître d'ouvrage" ; dans le sens du contrôle d'une force dynamique, l'expression "maîtrise de la vitesse" apparaît également dans le code de la route. Mais surtout, la définition que nous vous

---

(1) Liste prévue par l'article 371 du code pénal.

proposons s'inspire de la notion de "maître du fichier" retenue par l'article 2d) de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, adoptée le 28 janvier 1981 par le Conseil de l'Europe et qui fait partie intégrante de notre droit positif depuis le 5 octobre 1985.

Reprenant pour une part les termes mêmes de la convention, on entend aussi par "maître du système" : "toute personne physique ou morale, toute autorité publique, tout service ou tout organisme qui est compétent pour disposer du système ou pour décider de sa conception, de son organisation ou de ses finalités" (amendement n° 2, second alinéa).

Cette approche présente, à notre sens, le double mérite de permettre **l'identification de la personne qui subit un préjudice informatique**, à l'exclusion du tiers pour lequel il pourra en résulter un autre préjudice (1) et d'éviter que ne soient consignées dans la loi pénale les conséquences d'accords purement contractuels susceptibles d'intervenir entre le propriétaire d'un système et celui auquel il consent l'utilisation de ce système. Elle constitue également un pas en direction de l'harmonisation des législations, dans un domaine où l'efficacité des dispositifs répressifs dépend largement d'un renforcement de la coopération internationale.

La définition du "système de traitements automatisés de données" et celle du "maître du système" sont indissociables ; il n'y aura pas de système, sans maître du système. La notion de maîtrise et la clé de voute qui assure la cohésion d'éléments qui, sans elle, seraient épars.

B. La protection pénale ne joue qu'au bénéfice des "systèmes protégés"

Les travaux de l'Assemblée nationale montrent clairement que les députés ont entendu lier la constitution du délit d'intrusion dans un système, à l'existence d'une protection du système. Dans cette perspective, il a paru souhaitable à votre commission d'insister sur l'importance fondamentale que revêt la question de la sécurié et d'inscrire, dans la loi elle-même, l'exigence d'une protection des systèmes.

---

(1) Il y aura alors cumul d'infractions, le tiers pouvant, par exemple, porter plainte pour escroquerie.

. Il est indispensable de renforcer la sécurité physique et logique des systèmes

Les systèmes informatiques sont fragiles et vulnérables. Il importe, en conséquence, d'attirer l'attention des maîtres des systèmes et des utilisateurs de services informatiques sur les responsabilités qui sont les leurs.

Afin de renforcer la protection des données, il convient notamment de **contrôler l'accès aux systèmes** et de **garantir la confidentialité des données.**

La gestion des droits d'accès est souvent assurée par une partie du système d'exploitation lui-même, ce qui facilite la mise en place d'un contrôle centralisé et impose à chaque utilisateur de passer par le mécanisme de contrôle des accès avant de pouvoir entrer en liaison avec un quelconque fichier. Le mécanisme qui permet de reconnaître l'utilisateur est un **mot de passe,** un **code** ou encore un **badge magnétique**, associé à une identification de système ou même de fichier.

Outre **l'identification** de l'auteur, il faut également prévoir son **authentification** ; à défaut, n'importe qui utilisant le code d'une personne habilitée pourrait pénétrer un système. Différentes techniques permettent de faciliter cette procédure, depuis la rémission périodique ou aléatoire de certaines sessions jusqu'à la signature électronique.

La protection de la confidentialité des données peut également être assurée au moyen de leur **cryptage**. Cette technique consiste à rendre inintelligibles à tous, sauf à ceux qui détiennent la clé de l'algorithme, les données ainsi chiffrées ; elle est particulièrement utile pour les informations sensibles et sur les lignes de transmission (1).

Le plus souvent, par exemple, il conviendra également d'établir des contrôles, pour les données entrantes et pour les sorties d'états, d'opérer la vérification des traitements effectués, d'établir des procédures de conservation des traces des opérations enregistrées.

---

(1) La fabrication, la vente, l'acquisition, la détention et l'utilisation des moyens de cryptologie sont soumises à une procédure d'autorisation administrative, au même titre que les autres matériels de guerre dits de seconde catégorie, qui figurent sur la liste établie par le décret-loi du 18 avril 1939 modifié par le décret n° 86-250 du 18 février 1986 (JO 26 février 1986, p. 3018).

Ce rapide survol ne prétend pas être exhaustif ; il est simplement destiné à attirer l'attention sur l'importance **d'une meilleure information du public** (1) en matière de sécurité -le code d'une carte de crédit ne doit être divulguée sous aucun prétexte- et sur la nécessité **d'un renforcement des dispositifs de sécurité et des procédures de contrôle.**

. La sanction pénale est applicable aux seuls systèmes protégés

L'Assemblée nationale a entendu lier l'efficacité de la protection pénale contre l'entrée frauduleuse dans un système de traitements automatisés de données, à un niveau minimal de protection du système ; elle n'a cependant pas jugé utile de faire figurer cette précision dans le texte même de la proposition de loi.

Certes, l'emploi du vocable "frauduleusement" suppose que l'acte incriminé a été intentionnel, c'est-à-dire que le délinquant a eu préalablement connaissance qu'il n'avait pas le droit d'accéder au système ; on pourra toutefois regretter que la notion même de protection du système ne figure pas explicitement dans le dispositif proposé.

Il convient en effet de sensibiliser les maîtres des systèmes aux précautions qu'ils doivent prendre, sans pour autant prévoir que les dispositifs de sécurité devront être adaptés aux exigences des systèmes concernés, dans la mesure où il ne paraît pas possible de lier l'infraction au niveau de sécurité opposé aux fraudeurs.

Il est en revanche clair que devant la rédaction que vous propose votre commission, le juge appréciera l'efficacité des dispositifs de protection et qu'il en tiendra compte dans le prononcé de la peine, dans la mesure où **seul le système "protégé par des dispositifs de sécurité" serait alors visé par la loi** (art. 462-2-A, premier alinéa).

On rappellera, sur cette question précise de la sécurité, que l'article 29 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, va même jusqu'à engager la responsabilité pénale de celui qui, ordonnant ou effectuant un traitement d'informations nominatives, n'aurait pas pris "toutes les précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés" ; cette carence est punie d'un emprisonnement d'un à cinq ans et d'une amende de 20 000 francs à 2 000 000 de francs, ou de l'une de ces deux peines seulement.

---

(1) Il n'est pas rare de voir s'afficher sur l'écran le mot "bienvenue", sans que rien n'indique que l'on est dans un système "fermé".

Cette disposition, dont la portée est très considérable, n'est pas reprise dans la proposition de loi ; son application reste donc limitée aux seules données personnelles, elle vient toutefois, de ce seul fait, compléter l'incitation au renforcement de la sécurité des systèmes qui soustend le texte qui vous est soumis.

C. La protection des données plutôt que celle des informations

La proposition de loi adoptée par l'Assemblée nationale emploie indifféremment les termes d'"information" et de "donnée" ; or, ainsi que le rapporteur M. René André l'a lui-même précisé, "le statut de l'information en général" est "une question très controversée" qu'il paraît difficile de résoudre dans le cadre de ce texte (1).

Votre commission préfère s'en tenir à la notion de "donnée" (amendement n° 4), dont la portée a été définie par l'arrêtée du 22 décembre 1981, complété et modifié par les arrêtés du 30 décembre 1983 et du 30 mars 1987 : "la donnée est la représentation d'une information sous une forme conventionnelle destinée à faciliter son traitement".

La protection garantie à la donnée -formalisation d'une information- peut d'ailleurs être renforcée par la protection dont bénéficie, en tant que telle, l'information qu'elle contient, notamment au moyen des dispositions des articles 74 et suivants du code pénal (secrets de la défense nationale), des articles 378 (secret professionnel) et 418 (secret de fabrique) du code pénal, des dispositions de la loi du 16 juillet 1980 (renseignements économiques et techniques)...

Les réflexions qui sont actuellement en cours autour de l'idée d'une propriété de l'information, conduiront peut-être à modifier cette approche juridique traditionnelle ; en l'état actuel de notre droit, il n'a pas été jugé souhaitable d'accorder à l'information enregistrée une protection supérieure à celle dont bénéficie l'information qui n'est pas enregistrée.

D. Le principe de deux incriminations fondamentales

L'Assemblée nationale a retenu deux catégories d'infractions en matière informatique ; votre commission vous propose de suivre cette classification, mais d'en simplifier le contenu afin de rester dans le cadre strictement défini des délits spécifiques à l'informatique.

---

(1) V. rapport précité, p. 10.

. L'incrimination d'"accès ou de maintien frauduleux" dans un système de traitements automatisés de données

L'incrimination d'"accès frauduleux" définie par l'Assemblée est apparue satisfaisante, dans la mesure où elle permet de sanctionner tout accès frauduleux en tant que tel et quelles qu'en soient les conséquences.

Votre commission vous propose toutefois d'en modifier légèrement la rédaction afin d'**étendre l'infraction** au cas du fraudeur habilité à accéder à une partie d'un système qui, ayant eu frauduleusement accès à une partie non autorisée de ce système, s'y maintient en connaissance de cause, et au cas du fraudeur qui, ayant eu par hasard accès à un système fermé, s'y maintient volontairement tout en sachant qu'il n'y a pas droit (**art. 462-2, premier alinéa, amendement n° 3).**

Le second alinéa de l'article 462-2 qui est destiné à sanctionner la détérioration involontaire d'un élément du système à l'occasion d'un accès ou d'un maintien frauduleux n'a pas semblé devoir être modifié, sous réserve, pour des motifs plus haut explicités, de la substitution du mot "données" au mot "informations" (**art. 462-2, second alinéa, amendement n° 4).**

. Le piratage informatique

La volonté de l'Assemblée nationale de sanctionner ce qui est communément appelé le piratage informatique s'est traduite par deux dispositions qui distinguent entre :

- le sabotage d'un système (art. 462-3), action volontaire distincte des dommages involontaires prévus au 2e alinéa de l'article 462-2 ;

- et l'action sur les informations (art. 462-4 1er alinéa), par suppression, modification ou adjonction.

Votre commission estime que ces qualifications ne tiennent pas compte de la réalité du piratage informatique et de ses procédés les plus usuels.

Elle n'est pas davantage attirée par la formulation retenue par plusieurs législations étrangères qui en font une atteinte aux biens, alors que dans notre pays la nature de l'information reste une question préjudiciable.

Elle considère enfin que le **piratage relève d'un concept exclusif de tous les autres à ce jour retenus par notre droit pénal,**

et qui est lié à la nature même de l'informatique (1).

Le piratage est avant tout la prise d'un pouvoir, celui qui procure la disposition indue d'un système de traitements automatisés de données.

Sans utiliser la force, à distance, sournoisement, une place est assiégée, des brêches irréversibles y sont faites, la puissance change de camp sans même que l'on s'en aperçoive.

C'est pourquoi votre commission a préféré à toutes autres incriminations pour qualifier ces actes, la notion de "substitution volontaire au maître du système" (**art. 462-4** dans la rédaction proposée par **l'amendement n° 6**).

Cette substitution a pour objet le contrôle, total ou partiel, d'une ou plusieurs des fonctions que la définition que nous avons proposée à l'article 462-2-A, attribue au maître du système ; la puissance qui appartient à celui-ci sera exercée par un tiers qui n'y a pas droit. Le fraudeur emploiera cette puissance pour un résultat qui n'a pas à être pris en compte dans cette incrimination spécifique, même si, le plus souvent, ce détournement entre dans la réalisation d'un autre acte délictueux.

Le facteur temps revêt en la circonstance une importance qui aurait été inconcevable avant le développement de l'informatique. D'une part, la vitesse de commutation permet de commettre l'infraction en-deçà d'un instant de raison, d'autre part, la programmation de l'horloge interne du système autorise l'infraction "en temps différé". Ce caractère spécifique est pris en compte dans la définition de l'infraction qui vous est proposée par la commission.

A la différence du délit visé à l'article 462-2, le piratage devra reposer sur des actes volontaires qui en seront les moyens ; ils porteront sur les logiciels du système, ses données, ses constituants physiques ou ses liaisons. C'est pourquoi à un catalogue des *modus operandi* décrits dans les typologies de la délinquance informatique, votre commission a préféré un dispositif général s'appuyant précisément sur les lieux de passage obligé de cette délinquance que sont les logiciels, les données, les constituants physiques, les liaisons.

La combinaison des définitions formulées à l'article 462-2-A avec la qualification définie par le nouvel article 462-4, devrait permettre d'appréhender sous toutes ses formes, et d'une manière relativement simple, le phénomène complexe qui fait l'objet du présent rapport.

---

(1) V. François Salle in Projet, sept. oct. 1986 : "L'étendue et la diversité des domaines couverts par l'informatique en font un outil de puissance donc de pouvoir potentiel considérable pour ceux qui en ont la maîtrise".

Il appartiendra aux tribunaux d'apprécier, au cas par cas, la gravité des agissements en cause. Il faut leur réserver un large pouvoir d'appréciation en aggravant les peines par rapport à celles retenues par l'Assemblée nationale ; il vous est proposé de retenir des peines d'emprisonneemnt d'un an à cinq ans et une amende de 200 000 francs à 2 000 000 de francs, soit des peines équivalentes aux peines les plus lourdes prévues par la loi du 6 janvier 1978 en matière de traitements automatisés d'informations nominatives.

Il convient toutefois de souligner que de telles peines sont justifiées au regard des **risques très importants** que de tels agissements font courir aux maîtres des systèmes et des **préjudices considérables** qu'ils peuvent occasionner.

Afin de compléter ce dispositif, il vous est également proposé de **punir la tentative des deux délits** ainsi définis **des mêmes peines que le délit lui-même (art. 462-4 bis, amendement n° 7).**

E. La suppression du faux informatique

L'Assemblée nationale a souhaité incriminer le faux informatique (art. 462-4, second alinéa, et art. 462-5 pour l'usage de faux). Votre commission a jugé ces dispositions incompatibles avec la ligne qu'elle s'est fixée, à savoir **ne retenir que des délits spécifiquement informatiques (art. 462-5, amendement n° 8).**

Certes, de telles dispositions qui trouvent directement leurs origines dans la proposition initiale de M. Godfrain, ne sont pas dénuées d'intérêt, mais outre qu'elles se résument, en fait, en une extension de dispositions préexistentes du code pénal, elles introduisent dans notre droit le principe selon lequel les données informatiques ont la même valeur juridique que des écrits ; or, nous avons vu plus haut **les dangers d'une telle assimilation, tant au vu de l'état actuel des techniques informatiques qu'au regard du droit de la preuve.**

F. Le délit d'entente en vue de commettre un piratage informatique

Les "bricoleurs de génie" isolés constituent une menace pour les systèmes informatiques ; il apparaît toutefois que c'est grâce à la mise en commun de leurs connaissances que cette menace acquiert sa pleine efficacité. Or, ces dernières années ont vu fleurir les clubs de passionnés de l'informatique qui échangent les renseignements dont ils disposent et les techniques qu'ils ont mises au point.

En conséquence, il a paru opportun à votre commission de **punir les ententes** établies en vue de la préparation du délit de piratage informatique **(art. 462-6-A, amendement n° 9).**

En conséquence, il a paru opportun à votre commission de **punir les ententes** établies en vue de la préparation du délit de piratage informatique **(art. 462-6-A, amendement n° 9).**

Cette disposition est d'autant plus nécessaire que la délinquance informatique tend à s'organiser selon une hiérarchie complexe, au sommet de laquelle se trouvent des délinquants confirmés dont les intentions sont loin d'être seulement ludiques et qui utilisent les clubs de "hackers" pour tester l'efficacité des procédés qu'ils ont mis au point.

L'article 462-6-A qui vous est proposé est repris des dispositions de l'article 265 du code pénal qui incrimine les associations de malfaiteurs ; les peines sont toutefois abaissées à un emprisonnement d'un mois à trois ans et une amende de 2 000 francs à 500 000 francs ou l'une de ces deux peines seulement, afin de ne pas sanctionner trop lourdement les "hackers", tout en permettant **la mise en détention provisoire dans le cas de faits plus graves** commis par des délinquants chevronés dont on peut craindre qu'ils ne poursuivent leurs agissements frauduleux.

*

* *

Sous le bénéfice de ces observations et sous réserve des amendements qu'elle vous propose, la commission vous demande de bien vouloir adopter la proposition de loi qui vous est soumise.

TABLEAU COMPARATIF

Texte en vigueur ----	Texte de la proposition de loi ----	Texte adopté par l'Assemblée Nationale ----	Propositions de la Commission ----
CODE PENAL	Article premier.	Article unique..	Article unique..
Art.165.Abrogé par le décret du 12 avril 1848	L'article 165 du code pénal est rétabli dans la rédaction ci-après : « Est réputé écriture ou document au sens du présent chapitre tout enregistrement informatique. »	Dans le titre II du livre III du code pénal, il est créé, après le chapitre II, un chapitre III intitulé : "De certaines infractions en matière informatique" et comportant les articles 462-2, 462-3, 462-4, 462-5 et 462- 6 ainsi rédigés :	Dans le titre II du livre III du code pénal, il est inséré, après le chapitre II, un chapitre III ainsi intitulé : "De certaines infractions en matière *de systèmes de traitements automatisés de données".* "Art. 462-2 A - *Au sens du présent chapitre, on doit entendre par système de traitement automatisé de données, tout ensemble composé d'une ou plusieurs unités de traitement, de mémoires, de logiciels, de données, d'organes d'entrees-sorties , et de liaisons, qui concourent à un résultat déterminé, cet ensemble étant protégé par des dispositifs de sécurité.*

Texte en vigueur	Texte de la proposition de loi	Texte adopté par l'Assemblée Nationale	Propositions de la Commission
			Au sens de l'article 462-4 du présent code, on doit entendre par maître du système toute personne physique ou morale, toute autorité publique, tout service ou tout organisme qui est compétent pour disposer du système ou pour décider de sa conception, de son organisation ou de ses finalités".
	Art. 2.		
	Il est inséré dans le code pénal un article 371-1 rédigé ainsi qu'il suit :		
	« Quiconque sera, délibérément, entré sans droit dans tout ou partie d'un système de traitement de l'information sera puni d'un emprisonnement de deux mois à un an et d'une amende de 2.000 à 60.000 F ou de l'une de ces deux peines seulement. »	"Art. 462-2. . Quiconque aura frauduleusement accédé, directement ou indirectement, à un système de traitement automatisé de données sera puni d'un emprisonnement de deux mois à un an et d'une amende de 2 000 F à 50 000 F ou de l'une de ces deux peines.	"Art. 462-2. Quiconque frauduleusement aura accédé *ou se sera maintenu dans tout ou partie d'*un système... ...peines.

Texte en vigueur	Texte de la proposition de loi	Texte adopté par l'Assemblée Nationale	Propositions de la Commission
Art.372 .Pour toutes les infractions prévues aux articles 368 à 371, la tentative du délit sera punie comme le délit lui-même. Dans les cas prévus aux articles 368 à 370, l'action publique ne pourra être engagée que sur plainte de la victime, de son représentant légal ou de ses ayants droit.			
Dans les cas visés à l'article 368, le tribunal pourra prononcer la confiscation du matériel ayant servi à commettre l'infraction. Dans les cas visés aux articles 368 et 369, il pourra prononcer la confiscation de tout enregistrement ou document obtenu à l'aide d'un des faits prévus à l'article 368.		"Lorsqu'il en sera résulté soit la suppression ou la modification d'informations contenues dans le système, soit une altération du fonctionnement de ce système, l'emprisonnement sera de deux mois à deux ans et l'amende de 10 000 F à 100 000 F.	"Lorsqu'il ... modification de *données* contenues... ... à 100 000 F.
Dans les cas visés à l'article 370, il pourra prononcer la confiscation du support du montage. Dans les cas visés à l'article 371, il prononcera la confiscation des appareils ayant fait l'objet d'une des opérations énumérées par cet article en l'absence d'autorisation.		"Art. 462-3. . Quiconque aura, intentionnellement et au mépris des droits d'autrui, entravé ou faussé le fonctionnement d'un système de traitement automatisé de données sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 10 000 F à 100 000 F ou de l'une de ces deux peines.	"Art. 462-3-. *supprimé*

Texte en vigueur	Texte de la proposition de loi	Texte adopté par l'Assemblée Nationale	Propositions de la Commission
Art.381. Le vol simple ou sa tentative sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 1.000 F à 20.000 F ou de l'une de ces deux peines seulement.	Art. 3. Le premier alinéa de l'article 372 du code pénal est rédigé ainsi qu'il suit : « Pour toutes les infractions prévues aux articles 367 à 371-1, la tentative du délit sera punie comme le délit lui-même. »	"Art. 462-4. . Quiconque aura, intentionnellement et au mépris des droits d'autrui, supprimé ou modifié des informations contenues dans un système de traitement automatisé de données ou introduit des informations dans un tel système sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 5 000 F à 100 000 F ou de l'une de ces deux peines. "Lorsque la suppression, la modification ou l'introduction des informations aura consisté en une altération de la vérité de nature à causer un préjudice à autrui, l'emprisonnement sera d'un an à cinq ans et l'amende de 20 000 F à 200 000 F.	Art. 462-4 - *Quiconque, en tout ou partie, pendant quelque durée que ce soit, nonobstant le résultat obtenu, et au préjudice du maître d'un système de traitement automatisé de données, se sera intentionnellement substitué à lui, en agissant sur les logiciels du système, ses données, ses constituants physiques, ou ses liaisons, sera puni d'un emprisonnement d'un an à cinq ans et d'une amende de 20 000 F à 2 000 000F.* *Alinéa supprimé.* *"Art. 462-4 bis - La tentative des délits prévus par les articles 462-2 et 462-4 est punie des mêmes peines que le délit lui-même".*

Texte en vigueur	Texte de la proposition de loi	Texte adopté par l'Assemblée Nationale	Propositions de la Commission
		"Art. 462-5. Quiconque aura fait usage sciemment de documents reproduisant des informations introduites ou modifiées dans les conditions prévues par le second alinéa de l'article 462-4 sera puni d'un emprisonnement d'un an à cinq ans et d'une amende de 20 000 F à 200 000 F ou de l'une de ces deux peines.	"Art. 462-5. -*Supprimé.*
			"Art. 462-6 A - Quiconque aura participé à une entente établie en vue de la préparation concrétisée par un ou plusieurs faits matériels de l'infraction définie à l'article 462-4 sera puni d'un emprisonnement d'un mois à trois ans et d'une amende de 2 000 F à 500 000 F, ou de l'une de ces deux peines.
		"Art. 462-6. . Le tribunal pourra prononcer la confiscation des matériels appartenant au condamné et ayant servi à commettre les infractions prévues au présent chapitre."	"Art. 462-6. -Sans modification.
	Art. 4. L'article 401 du code pénal est complété par un sixième alinéa rédigé ainsi qu'il suit :		

Texte en vigueur	Texte de la proposition de loi	Texte adopté par l'Assemblée Nationale	Propositions de la Commission
Art.401. Quiconque, sachant qu'il est dans l'impossibilité absolue de payer, se sera fait servir des boissons ou des aliments qu'il aura consommés, en tout ou en partie, dans des établissements à ce destinés même s'il est logé dans lesdits établissements, sera puni d'un emprisonnement de six jours au moins et de six mois au plus, et d'une amende de 500 F au moins et de 15000 F au plus..			
La même peine sera applicable à celui qui, sachant qu'il est dans l'impossibilité absolue de payer, se sera fait attribuer une ou plusieurs chambres dans un hôtel ou auberge et les aura effectivement occupées			
Toutefois, dans les cas prévus par les deux alinéas précédents, l'occupation du logement ne devra pas avoir excédé une durée de dix jours.			
Sera passible des mêmes peines quiconque, sachant qu'il est dans l'impossibilité absolue de payer, se sera fait servir des carburants ou lubrifiants dont il aura fait remplir en tout ou partie les réservoirs d'un véhicule par des professionnels de la distribution.			

Texte en vigueur	Texte de la proposition de loi	Texte adopté par l'Assemblée Nationale	Propositions de la Commission
....	....	....	....
	«Sans préjudice de l'application des peines plus graves prévues par les dispositions du présent code ou ses lois spéciales, quiconque, aura capté délibérement, sans droit, des données ou des programmes enregistrés, sera puni des peines portées en l'article 381.»		
	Art. 5.		
	Le premier alinéa de l'article 405 du code pénal est rédigé ainsi qu il suit :		
	« Quiconque, soit en faisant usage de faux noms ou de fausses qualités, soit en faisant indûment usage d'un code d'identification ou d'accès, soit en employant des manœuvres frauduleuses pour		

Texte en vigueur	Texte de la proposition de loi	Texte adopté par l'Assemblée Nationale	Propositions de la Commission
Art.405.Quiconque, soit en faisant usage de faux noms ou de fausses qualités, soit en employant des manoeuvres frauduleuses pour persuader l'existence de fausses entreprises, d'un pouvoir ou d'un crédit imaginaire, ou pour faire naître l'espérance ou la crainte d'un succés, d'un accident ou de tout autre évènement chimérique, se sera fait remettre ou délivrer, ou aura tenté de se faire remettre ou délivrer des fonds, des meubles ou des obligations, dispositions, billets, promesses, quittances ou décharges, et aura, par un un de ces ces moyens escroqué ou tenté d'escroquer la totalité ou partie de la fortune d'autrui, sera puni d'un emprisonnement d'un an au moins et de cinq ans au plus , et d'une amende de 3.600 F au moins et de 36.000 F francs au plus . Si le délit a été commis par une personne ayant fait appel au public en vue de l'émission d'actions, obligations bons, parts, ou titres quelconques, soit d'une société , soit d'une entreprise commerciale ou industrielle, l'emprisonnement pourra ître porté à dix années et l'amende à 180.000 F .	persuader l'existence de fausses entreprises, d'un pouvoir ou d'un crédit imaginaire, ou pour faire naître l'espérance ou la crainte d'un succès, d'un accident ou de tout autre événement chimérique, se sera fait remettre ou délivrer, ou aura tenté de se faire remettre ou délivrer des fonds, des meubles, des obligations. dispositions, billets, promesses, quittances ou décharges, ou des données ou programmes enregistrés, et aura, par un de ces moyens, escroqué ou tenté d'escroquer la totalité ou partie de la fortune d'autrui, sera puni d'un emprisonnement d'un an au moins et de cinq ans au plus, et d'une amende de 3.600 F au moins et de 2.500.000 F au plus. »		

Texte en vigueur	Texte de la proposition de loi	Texte adopté par l'Assemblée Nationale	Propositions de la Commission
Dans tous les cas, les coupables pourront être, en outre, frappés pour dix ans au plus de l'interdiction des droits mentionnés en l'article 42 du présent code.			
	Art. 6.		
	Le premier alinéa de l'article 408 du code pénal est rédigé ainsi qu'il suit :		
Art. 408. Quiconque aura détourné ou dissipé au préjudice des propriétaires, possesseurs ou détenteurs, des effets, deniers, marchandises, billets, quittances ou tous autres écrits contenant ou opérant obligation ou décharge, qui ne lui auraient été remis qu'à titre de louage, de dépôt de mandat, de nantissement, de prêt à usage, ou pour un travail salarié ou non-salarié, à la charge de les rendre ou représenter, ou d'en faire un usage ou un emploi déterminé, sera puni des peines portées en l'article 406.	« Quiconque aura détourné ou dissipé, au préjudice des propriétaires, possesseurs ou détenteurs, des effets, deniers, marchandises, billets, quittances ou tous autres écrits contenant ou opérant délégation ou décharge, ou des données ou programmes enregistrés, qui ne lui auraient été remis qu'à titre de louage, de dépôt, de mandat, de nantissement, de prêt à usage, ou pour un travail salarié ou non salarié, à la charge de les rendre ou représenter, ou d'en faire un usage ou un emploi déterminé, sera puni des peines portées en l'article 406 du code pénal. »		

Texte en vigueur	Texte de la proposition de loi	Texte adopté par l'Assemblée Nationale	Propositions de la Commission
Si l'abus de confiance a été commis par une personne faisant appel au public afin d'obtenir, soit pour son propre compte, soit comme directeur, administrateur ou agent d'une société ou d'une entreprise commerciale ou industrielle, la remise de fonds ou valeurs à titre de dépôt, de mandat ou de nantissement, la durée de l'emprisonnement pourra être portée à dix ans et l'amende à 5 000 000 de francs. Les dispositions portées au dernier alinéa de l'article 405 pourront de plus être appliquées.			
Les alinéas 2 et 3 du présent article sont applicables si l'abus de confiance a été commis par un courtier, un intermédiaire, un conseil professionnel ou un rédacteur d'actes et a porté sur le prix de vente d'un immeuble ou d'un fonds de commerce, le prix de souscription, d'achat ou de vente d'actions ou de parts de sociétés immobilières, ou sur le prix de cession d'un bail lorsqu'une telle cession est autorisée par la loi ou sur tout ou partie des sommes recouvrées pour le compte d'autrui.			

Texte en vigueur	Texte de la proposition de loi	Texte adopté par l'Assemblée Nationale	Propositions de la Commission
Si l'abus de confiance prévu à l'alinéa 1er a été commis par un officier public ou ministériel, la peine sera celle de la réclusion criminelle à temps de cinq à dix ans.			
Le tout, sans préjudice de ce qui est dit aux articles 254, 255 et 256, relativement aux soustractions et enlèvements de deniers, effets ou pièces, commis dans les depôts publics			
	Art. 7.		
	Le premier alinéa de l'article 434 du code pénal est rédigé ainsi qu'il suit :		
Art. 434. Quiconque aura, volontairement, détruit ou détérioré un objet mobilier ou un bien immobilier appartenant à autrui, sera, sauf s'il s'agit de détériorations légères, puni d'un emprisonnement de trois mois à deux ans et d'une amende de 2.500 F à 50.000 F ou de l'une de ces deux peines seulement.	« Quiconque aura, volontairement, détruit ou détérioré un objet mobilier, une donnée ou un programme enregistré ou bien immobilier appartenant à autrui, sera, sauf s'il s'agit de détériorations légères, puni d'un emprisonnement de trois mois à deux ans et d'une amende de 2.500 à 50.000 F ou de l'une de ces deux peines seulement. »		
Lorsque la destruction ou la détérioration aura été commise avec effraction, l'emprisonnement sera d'un an à quatre ans et l'amende de 5.000 F à 100.000 F.			
Il en sera de même :			

Texte en vigueur	Texte de la proposition de loi	Texte adopté par l'Assemblée Nationale	Propositions de la Commission
1° Lorsque l'infraction aura été commise au préjudice d'un magistrat, d'un juré ou d'un avocat, en vue d'influencer son comportement dans l'exercice ou à l'occasion de l'exercice de ses fonctions ;			
2° Lorsque l'infraction aura été commise au préjudice d'un témoin, d'une victime ou de toute autre personne, soit en vue de les déterminer à ne pas dénoncer les faits, à ne pas porter plainte, à ne pas faire de déposition, ou à faire une déposition mensongère, soit en raison de la dénonciation, de la plainte ou de la déposition.			
	Art. 8.		
	Les deux premiers alinéas de l'article 439 du code pénal sont rédigés ainsi qu'il suit :		
Art. 439. Quiconque aura volontairement brulé ou détruit, d'une manière quelconque, des registres, minutes ou actes originaux de l'autorité publique, des titres, billets, lettres de change, effets de commerce ou de banque, contenant ou opérant obligation, disposition ou décharge ;	« Quiconque aura volontairement brûlé ou détruit, d'une manière quelconque, des registres, minutes ou actes originaux de l'autorité publique des titres, billets, lettres de change, effets de commerce ou de banque, enregistrements informatiques, contenant ou opérant obligation, disposition ou décharge ;		

Texte en vigueur	Texte de la proposition de loi	Texte adopté par l'Assemblée Nationale	Propositions de la Commission
Quiconque aura sciemment détruit, soustrait, recélé, dissimulé ou altéré un document public ou privé de nature à faciliter la recherche des crimes et délits, la découverte des preuves ou le chatiment de leur auteur sera, sans préjudice des peines plus graves prévues par la loi, puni ainsi qu'il suit :	« Quiconque aura sciemment détruit, soustrait, recelé, dissimulé ou altéré un document public ou privé ou un enregistrement informatique de nature à faciliter la recherche des crimes et délits, la découverte des preuves ou le châtiment de leur auteur sera, sans préjudice des peines plus graves prévues par la loi, puni ainsi qu'il suit. »		
Si les pièces détruites sont des actes de l'autorité publique, ou des effets de commerce ou de banque, la peine sera la réclusion criminelle à temps de cinq à dix ans			
S'il s'agit de toute autre pièce, le coupable sera puni d'un emprisonnement de deux à cinq ans et d'une amende de 500 F à 8.000 F.			

Imprimerie du Sénat