DIRECTION GENERALE DES IMPOTS

ECOLE NATIONALE DES IMPOTS

INFORMATIQUE

FASCICULE 5

Traitements informatisés

Sécurité - Fiabilité - Contrôle

Avril 1982

TABLE DES MATIERES

CHAPITRE X

SECURITE ET FIABILITE DES TRAITEMENTS INFORMATISES

SECTION I

GENERALITES

Les performances de l'ordinateur sont telles que l'on pourrait penser que le traitement automatisé de l'information devrait être plus fiable que le traitement manuel. Pourtant, cette machine, qui a les défauts de ses qualités, reste un outil potentiellement dangereux, capable du meilleur et du pire, suivant l'usage qui en est fait.

En dehors des erreurs involontaires dues à une mauvaise maîtrise des techniques d'exploitation, les exemples de manipulation ou de fraudes à l'aide ou au travers de l'ordinateur, peuvent être nombreuses et variées, l' imagination des fraudeurs étant décuplée par la puissence de la machine.

On peut essayer de classer les menaces qui pèsent sur le traitement informatisé selon plusieurs critères.

1 - Critère de sécurité générale

- Agression
  - Naturelle (feu, eau ...,
  - Sabotage ou infraction
  - Sociale (destruction par malveillance)
- Destruction
  - Physique (accidentelle ou volontaire)
  - Informatique (accidentelle ou volontaire)
- Défaillance
  - Matériel
  - Logiciel
- Erreur
  - Humaine
  - Due au matériel
  - Due au logiciel
- Vol
  - De matériel
  - D'information
  - De programme
- Fraude
  - Sur les informations
  - Sur les traitements

2 - Critère du secret de l'information

- Vol
  - de matériel : supports
  - d'informations : Duplication, listings documents, fichiers ...
- Consultation illicite
  - Listings
  - Documents
  - Fichiers

  (volontaire (espionnage) / involontaire (erreur de manipulation))

3 - Critère de la sûreté de fonctionnement

- Vulnérabilité
  - des moyens de production
  - des systèmes d'exploitation
- Pannes
  - matériel
  - logiciel
  - social : grève
- Erreurs d'information
  - utilisation de mauvais fichiers

Dans une deuxième approche on peut classer ces fraudes en deux catégories selon leur origine,

- les fraudes ou manipulations effectuées à l'insu de l'entreprise
- les fraudes organisées par l'entreprise.

I - LES FRAUDES OU MANIPULATIONS EFFECTUEES A L'INSU DE L'ENTREPRISE

Elles sont la conséquence directe de l'utilisation de la machine, de ses possibilités et de son aspect "fermé", réservé aux spécialistes ou aux "bricoleurs" astucieux. Elles ont plusieurs origines.

1 - Les fraudes dues à une insuffisance de l'organisation

Souvent l'origine de la fraude réside dans une mauvaise séparation des fonctions de programmeurs et d'opérateurs et dans un contrôle insuffisant des programmes utilisés. L'accès à l'ordinateur doit être contrôlé et toute opération doit obligatoirement être répertoriée.

Si ces grands principes ne sont pas respectés les possibilités de fraudes sont très grandes. Les exemples sont nombreux :

- une banque américaine a été délestée de près de 100 millions de francs grâce à une utilisation frauduleuse de son ordinateur par un employé indélicat

- Une grande compagnie d'assurances a subi un préjudice très important au bénéfice d'un petit groupe de cadres qui avaient introduit dans les fichiers de l'ordinateur plusieurs dizaines de milliers de clients fictifs auxquels étaient versées des indemnités

- Un programmeur qui désirait doubler sa paie met au point un mécanisme astucieux pour arriver à ses fins

- Un autre, chargé d'automatiser le traitement des opérations financières d'une banque et notamment la liste des clients ayant un découvert donne l'ordre à la machine de ne pas signaler le découvert de son propre compte.

On pourrait multiplier les exemples. Les défauts dans la conception des applications et la faiblesse du contrôle interne en sont les principales causes.

2 - Les malversations qui ont leur origine à l'extérieur de l'entreprise

Les exemples sont également nombreux et variés

- de jeunes lycéens, grâce au mini-ordinateur de leur école relié à un réseau de télétraitement, découvrent par tâtonnement le code d'accès à une grande banque de données canadienne. Pendant plusieurs mois ils sont ainsi accès à ces informations, pouvant les altérer ou en introduire d'autres.

- Un programmeur mécontent de son licenciement se venge en ordonnant à l'ordinateur de détruire, plusieurs mois après son départ, toutes les mémoires de l'ordinateur (technique dite des bombes à retardement).

- Le vol de fichiers magnétiques est également pratiqué. Il sont soit vendus à un concurrent, soit échangés contre rançon.

Enfin les plastiquages et destruction de centres de traitement informatisés sont relativement fréquents.

Une étude publiée dans la revue Informatique et Gestion de novembre 1979 répartit ces délits de la façon suivante :

- Actes de destruction	19 %
- Vols de temps machine ou de service informatique	15 %
- Vol d'information	23 %
- Détournements de biens et de fonds	43 %
	100 %

Les possibilités de fraude ou de malversation existent à tous les niveaux : conception, programmation, saisie des données, traitement, stockage. Le développement de telles pratiques se trouvera facilité avec l'utilisation de plus en plus répandue du télétraitement. Les points d'accès à l'ordinateur étant multipliés et éparpillés dans l'espace.

Dans ce contexte la sécurité est entrain de devenir la priorité numéro un des utilisateurs de l'informatique. A l'occasion du premier colloque européen sur la sécurité des ordinateurs, réuni en janvier 1981 à Monté-Carlo, les experts internationaux ont manifesté leurs craintes : la révolution informatique, ont-il reconnu, a créé une nouvelle race de malfaiteurs rompus aux algorithmes et au système binaire. A la lumière de leurs travaux on commence à s'apercevoir que le code d'un ordinateur est peut être plus facile à percer qu'on ne le pense. La presse spécialisée et les publications comptables consacrent de nombreux articles à ce problème.

Malgré les précautions prises et qui devront être développées : ordinateurs sous bonne garde, contrôle de ceux qui ont accès à la machine par code, carte magnétique, badge ou mot de passe, fichiers gardés en double exemplaire et dans des coffres, les risques sont encore grands.

Si une entreprise souhaite avoir toutes confiance dans ses traitements informatiques elle doit respecter impérativement les principes du contrôle interne que l'on peut définir comme "l'ensemble des sécurités contribuant à la maîtrise de l'entreprise. Il a pour but, d'un côté, d'assurer la protection, la sauvegarde du patrimoine, et la qualité de l'information, de l'autre, l'application des instructions de la direction et de favoriser l'amélioration des performances". *

Une révision, c'est-à-dire un examen périodique effectué par un spécialiste compétent et indépendant doit compléter le contrôle interne. Le réviseur ou audit informatique procède à des opérations de vérification, de diagnostic, qui ont pour but de s'assurer que le service informatique fonctionne de façon sûre et efficace conformément aux règles normales permettant de garantir la sincérité et la régularité de la comptabilité.

II - LA FRAUDE ORGANISEE PAR L'ENTREPRISE

Si l'ordinateur est un merveilleux outil d'aide à la gestion il est également un formidable instrument de fraudes. Celles-ci se rapprochent tout naturellement des fraudes fiscales traditionnelles. Mais leur détection se complique du fait de l'utilisation de l'ordinateur avec son langage spécifique, son travail interne qui ne laisse aucune trace et ses supports de l'information illisibles directement par l'homme.

De ce fait l'attitude du vérificateur devant une comptabilité informatisée devra être différente de celle traditionnellement observée en présence d'une comptabilité tenue manuellement.

---

* Définition proposée par l'Ordre des Experts-Comptables et des Comptables Agréés.

Les comptabilités informatisées peuvent être classées en trois grands types suivant le mode d'utilisation de l'ordinateur.

1) Les comptabilités confiées en sous-traitance à des sociétés de services. Les façonniers disposent généralement de moyens de traitement puissants et de programmes généraux susceptibles de traiter les dossiers de tous leurs clients. Ceux-ci font parvenir leurs données soit par bordereaux de saisie manuels, soit par supports informatiques : cartes, bandes magnétiques, disques, disquettes ..., ils peuvent également utiliser le télétraitement.

Ce type de comptabilité est fréquemment rencontré dans les petites et moyennes entreprises. Elles peuvent être contrôlées suivant les règles traditionnelles, par rapprochement des états comptables et des pièces justificatives et sans qu'il soit indispensables, en principe, d'analyser le processus d'entrée et de traitement des données. D'ailleurs le client ignore généralement tout de ce processus.

2) Les comptabilités informatisées de type traditionnel éditées par les propres ordinateurs des entreprises. L'analyse de conception reste relativement simple mais la difficulté provient du nombre de mouvements. Si les procédures habituelles de contrôles restent encore applicables, le vérificateur devra également s'intéresser à la qualité du travail effectué par l'ordinateur.

3) Les systèmes dits "intégrés" dans lesquels la comptabilité générale ne devient qu'un sous produit de la gestion. Le système consiste, au moins en première approximation à saisir le plus près possible de leur source toutes les informations élémentaires nécessaires à la gestion en vue de les transmettre à l'unité centrale dont le logiciel très évolué les soumet à un traitement hautement sophistiqué qui fournit sans délai l'ensemble des renseignements nécessaires à la gestion.

Des volumes considérables de données sont manipulés sans édition d'états : il en résulte que le système traditionnel de référence a généralement disparu. Le système soulève par l'immatérialité même de sa production des problèmes graves liés à la fiabilité des écritures comptables et aux problèmes de contrôles externes.

SECTION II

LA PRODUCTION ET LA CONSERVATION DES DOCUMENTS COMPTABLES

LE PROBLEME DE LA PREUVE

Malgré l'évolution du mode de traitement des données comptables, le législateur n'a pas modifié les obligations des personnes astreintes à la tenue d'une comptabilité et les dispositions prévues par le Code de Commerce gardent toute leur valeur.

En effet, quel que soit le système adopté par l'entreprise - manuel, mécanographique, informatique - la comptabilité doit toujours présenter à l'égard des tiers, dont l'Administration, des garanties et notamment un caractère probant, ce qui implique la possibilité de reconstituer et de suivre dans toutes ses phases le traitement d'une donnée de base, depuis sa prise en charge par l'ordinateur jusqu'à sa restitution sous la forme d'un résultat.

Cette possibilité matérielle de reconstitution exige deux éléments : l'existence physique de documents comptables et leur lisibilité. Or le traitement des données peut affecter l'un et l'autre . Les supports magnétiques ou microfilmés n'offrent pas les mêmes garanties que le support papier et l'usage systématique de codes astreint le vérificateur à se reporter à une clé pour analyser et comprendre le système comptable.

Disponibilité et lisibilité ne sont cependant pas les seules garanties que doit offrir une comptabilité. En effet, le vérificateur doit permettre de s'assurer que les mentions portées dans les documents sont exactes, traduisent fidèlement les faits juridiques et retracent l'ensemble des opérations de l'entreprise. Si ces contrôles, pour des raisons de présentation des supports, ne peuvent être opérés, la preuve de l'exactitude, de la sincérité et du caractère probant de la comptabilité ne peut être apportée, ce qui en droit fiscal français signifie que l'Administration a la possibilité d'en contester les résultats.

Fort heureusement, la doctrine comptable par l'intermédiaire du Conseil national de la Comptabilité, par les publications de l'Ordre des Experts-Comptables et les recommandations du Conseil National des Commissaires aux Comptes est venue s'enrichir des normes auxquelles doivent satisfaire les comptabilités tenues sur ordinateur pour être régulières en la forme et pour offrir les garanties pour un contrôle a posteriori.

I - RECOMMANDATION DU CONSEIL NATIONAL DE LA COMPTABILITE

Publiée en 1976 cette recommandation a été intégralement reprise dans le Titre I, chapitre I du projet de Plan Comptable révisé. Elle stipule :

1) L'organisation du système de traitement doit garantir toutes les possibilités d'un contrôle éventuel.

2) Le système de traitement doit établir, sur papier ou éventuellement sur tout support offrant les conditions de garantie et de conservation définies en matière de preuve, des états périodiques numérotés et datés récapitulant dans un ordre chronologique toutes les données qui y sont entrées, sous une forme interdisant toutes insertions intercalaires ainsi que toutes suppressions ou additions ultérieures.

3) L'origine, le contenu et l'imputation de chaque données doivent être indiqués en clair. En outre, chaque donnée doit s'appuyer sur une pièce justificative constituée par un document écrit.

Lorsque les données sont prises en charge par un procédé qui, autrement, ne laisserait aucune trace, elles doivent être également constatées par un document écrit directement intelligible.

4) Il doit être possible, à tout moment, de reconstituer à partir des données définies ci-dessus les éléments de comptes, états et renseignements, soumis à la vérification ou, à partir de ces comptes, états et renseignements, de retrouver les données entrées.

C'est ainsi que tout solde de compte doit pouvoir être justifié par un relevé des écritures dont il procède à partir d'un autre solde de ce même compte. Chacune de ces écritures doit comporter une référence permettant l'identification des données correspondantes.

5) L'exercice de tout contrôle doit comporter droit d'accès à la documentation relative aux analyses, à la programmation et à l'exécution des traitements en vue de procéder notamment aux tests nécessaires.

6) Les procédures de traitement automatisé des comptabilités doivent être organisées de manière à permettre de contrôler si les exigences de sécurité et de fiabilité requises en la matière ont bien été respectées.

II - RECOMMANDATION DU CONSEIL NATIONAL DES COMMISSAIRES AUX COMPTES

Dans sa recommandation N° 38 le Conseil National des Commissaires aux Comptes a proposé un certain nombre de solutions pratiques dont voici quelques extraits :

Contrôle des comptabilités traitées par des moyens informatiques.

L'exigence d'une gestion de plus en plus précise, la taille et la complexité des ensembles industriels et financiers, les politiques de décentralisation caractérisent l'économie moderne.

Il en résulte que :

- l'information est saisie à son niveau le plus petit et doit pouvoir faire l'objet de classements et de traitements nombreux et rapides ayant chacun des objectifs particuliers ;

- la quantité d'informations à traiter exclut les méthodes anciennes.

L'informatique est une réponse à ces besoins mais on constate que :

- sa haute technicité conduit à la réserver à des spécialistes ;

- les services informatiques protégés par leur technicité sont souvent incontrôlés ;

- les besoins comptables élémentaires et les règles de sécurité sont parfois méconnus ou négligés ;

- les progrès du matériel et leur changement rendent parfois impossibles les contrôles à postériori ;

- les programmes de contrôle souvent complexes inclus dans les traitements ne détectent que les cas d'erreurs qui ont été prévus lors de leur conception.

Il importe donc de rechercher quelles sont les règles indispensables pour :

- assurer la fiabilité des résultats produits ;

- permettre de satisfaire aux exigences du droit commercial, du droit fiscal et de la prévention des malversations.

Dans ce but il convient d'examiner :

- quelles sont les règles qui donnent à une comptabilité sa force probante ;

- quelles sont les méthodes pratiques qui permettent de s'assurer du bon fonctionnement d'un service de traitement des données.

1 - Règles donnant à une comptabilité sa force probante

On doit distinguer deux types de règles :

- les règles issues de la loi ou du règlement ;

- les règles issues de la pratique.

a) Les règles de droit.

L'article 9 du code de commerce impose la tenue d'un livre-journal enregistrant au jour le jour les opérations ou récapitulant au moins mensuellement les totaux de ces opérations en conservant dans ce cas les documents permettant de vérifier les opérations jour par jour.

Par ailleurs, un ensemble de textes législatifs ou règlementaires a défini des règles de classement, d'évaluation, ou de comptabilisation (loi du 24 juillet 1966, décret du 23 mars 1967, Plan comptable général et plans comptables professionnels).

b) Les règles pratiques.

La pratique comptable a permis d'élaborer un certain nombre de règles ayant pour but d'accroître la sécurité des enregistrements comptables et d'en faciliter le contrôle.

- Le contrôle de la validité de l'enregistrement élémentaire implique qu'il soit possible de revenir à la pièce justificative.

- Le contrôle de la comptabilité proprement dite implique que l'organisation de cette comptabilité soit telle que l'on puisse s'assurer :

- que toutes les informations saisies dans les comptes sont identiques à celles des journaux (égalité des mouvements des journaux avec ceux du Grand Livre) ;

- que les liaisons entre les états récapitulatifs et l'information élémentaire sont assurées.

2 - Conséquences de ces règles sur les traitements informatiques

On peut résumer les conditions fondamentales de fiabilité comme suit :

- toutes les informations entrées dans un système informatique doivent pouvoir être contrôlées et faire l'objet d'états imprimés (liste de contrôle ou journaux) ; lorsqu'il s'agit de mouvements exprimés en quantité valorisée par l'ordinateur au moyen de tables de valorisation, l'historique des tables de valorisation doit être conservé ;

- on doit pouvoir s'assurer que toutes les informations nécessaires à la fiabilité d'un document financier ont été traitées ; les contrôles en mouvement doivent être possibles et pas seulement les contrôles en solde ;.

- les informations entrées dans un système informatique doivent pouvoir être recoupées avec les pièces justificatives ;

- il doit être possible, dans la limite des prescriptions légales, d'obtenir des états imprimés donnant l'historique et la position des comptes financiers à un moment donné ;

- on doit pouvoir s'assurer que le système fonctionne convenablement, d'où l'importance du contrôle interne.

III - POSITION DE LA DIRECTION GENERALE DES IMPOTS

Ces problèmes n'ont pas échappé à l'Administration fiscale, qui a provoqué dès 1976 la création d'une "commission informatique" laquelle a publié la recommandation du Conseil national de la comptabilité (voir B.O.D.G.I. 13 K-4-1976). Dans son article 97 la loi de Finances pour 1982 apporte les modifications suivantes à l'Article 54 du C.G.I. :

"I - Si la comptabilité est établie au moyen de systèmes informatisés, le contrôle s'étend à la documentation relative aux analyses, à la programmation et à l'exécution des traitements. Afin de s'assurer de la fiabilité des procédures de traitement automatisé de la comptabilité, les agents des Impôts peuvent procéder à des tests de contrôle sur le matériel utilisé par l'entreprise dont les conditions seront définies par décret."

II - Lorsqu'une vérification de comptabilité, une procédure de redressement ou l'instruction d'une réclamation formulée par le contribuable requiert des connaissances techniques particulières, l'administration pourra faire appel aux conseils techniques d'agents de l'Etat ou des établissements publics figurant sur une liste arrêtée par le ministre délégué auprès du ministre de l'économie et des finances, chargé du budget.

Cette disposition n'est applicable qu'aux entreprises ainsi que, le cas échéant, à leurs mères et filiales, dont le chiffre d'affaires total dépasse 20 000 000 F.

Les agents ainsi désignés sont tenus au secret professionnel dans les termes de l'article L 103 du livre des procédures fiscales du nouveau code des impôts."

Le vérificateur de comptabilité ne peut pas ignorer les changements qui affectent les conditions d'exercice de ses fonctions. Il devra utiliser pleinement les possibilités que lui offrent les textes pour surmonter les réticences des entreprises et ne pas hésiter à soumettre les cas douteux à l'appréciation des tribunaux, l'évolution et l'application des textes existants dépendant très largement des orientations de la jurisprudence.

SECTION III

ATTITUDE DU VERIFICATEUR
FACE AUX COMPTABILITES INFORMATISEES

L'application des moyens et des procédures informatiques de traitement des comptabilités oblige le vérificateur à incorporer dans son plan de travail l'examen et l'appréciation de la qualité et de la sécurité des prestations fournies par ces techniques.

Le développement des méthodes informatiques dans la gestion des entreprises met particulièrement en évidence la nécessité, pour le vérificateur, d'analyser logiquement la conception et le fonctionnement du système de traitement. Il devra adapter ses procédures de contrôle à la nouvelle présentation des informations qui ne sont pas systématiquement mises sur des supports "en clair".

La façon d'exécuter sa mission s'écartera d'autant plus des techniques de contrôles traditionnelles que le système de traitement informatisé sera plus développé.

Il n'est pas possible ici, de définir, avec précision, les modalités d'intervention du vérificateur devant de telles situations. Une mission d'études sur ce problème a été créée à la D.G.I. en 1980.

Suite à son rapport, la création d'une brigade de vérification spécialisée a été décidée. Elle sera composée de 6 agents : 2 analystes, 1 programmeur, 3 vérificateurs placés sous l'autorité d'un chef de brigade. Elle sera rattachée directement à la Sous-Direction II B et devra être opérationnelle au 4e trimestre 1982.

Dans un premier temps elle interviendra, à la demande de la Mission de Coordination du Contrôle Fiscal, sur la région Ile-de-France.

Après une expérience d'environ 2 ans un premier bilan d'activité sera tiré. S'il est positif le développement de ce type de brigade pourrait être envisagé.

Suivant le type de comptabilité et le niveau de son intervention l'attitude du vérificateur sera différente.

I - LES RECOUPEMENTS

Cette phase du travail, indispensable à la vérification, ne doit pas subir de modification importante, qu'on soit ou non en présence d'une comptabilité informatisée. Toutefois deux observations peuvent être formulées.

1) L'exercice du droit de communication peut être rendu difficile par des arguments du type "mon système d'exploitation ne me permet pas de sortir "en clair" la situation de tel compte client" ou "toutes mes archives sont sur bandes magnétiques ou sur microfiches...". Ce genre d'arguments risque de se rencontrer de plus en plus fréquemment. Bien entendu le vérificateur ne devra pas, pour ces motifs, renoncer à exercer les droits de communication et de vérification qu'il détient en vertu des dispositions du C.G.I.

2) Il est vraisemblable que le vérificateur pourra obtenir des C.R.I. un certain nombre de renseignements qui lui faciliteront son travail de recoupement. Des expériences ont été tentées dans ce sens : on a extrait du R.C.M.E. soit d'un département, soit d'une région toutes les entreprises exerçant une profession déterminée. Cette liste, par rapprochement avec le fichier clients de l'entreprise vérifiée, a permis, après recoupements, de découvrir que tous les clients de l'entreprise n'étaient pas pris en compte dans sa comptabilité.

La création d'un fichier des entreprises à partir du R.C.M.E. simplifié est envisagée. D'un accès facile il permettra par rapprochement avec les fichiers clients et fournisseurs de l'entreprise vérifiée de mettre en évidence l'existence éventuelle d'entreprises qui travaillent "au noir" ou d'entreprises émettrices de factures sans contrepartie réelles (système "taxi").

II - LE CONTROLE DES COMPTABILITES TRAITEES PAR UN FACONNIER

La vérification des moyens et des méthodes de traitement informatisés de la comptabilité par le façonnier n'est pas possible ici. Il s'ensuit que la vérification doit être conduite suivant les normes traditionnelles tout en s'adaptant à la nouvelle présentation des documents.

Le vérificateur devra exiger un certain nombre de renseignements tels que Plan Comptable de l'entreprise, éléments de codification... Il devra obligatoirement avoir la liste des pièces de base prises en compte par le façonnier (liste d'entrée des données).

Il devra également connaître la procédure de transmission des données : type de support (bordereaux, bandes magnétiques...) ; le mode de prise en charge par le façonnier. Il recherchera ensuite la nature des traitements effectués (contrats ou cahiers des charges). Enfin, afin de se faire une idée précise sur la qualité des documents qui lui sont remis, il devra s'informer sur la nature et la fréquence des contrôles qui sont effectués tant sur les entrées qu'en cours de traitement (voir en annexe quelques exemples de contrôles effectués par un façonnier sur les entrées par bordereaux manuels ou optiques).

III - LE CONTROLE DE LA COMPTABILITE TENUE PAR LE PROPRE ORDINATEUR DE L'ENTREPRISE

Si les façonnier utilisent des programmes généraux applicables à tous leurs clients les entreprises qui disposent d'un ordinateur ont leurs propres programmes, ce qui multiplie les possibilités d'erreurs, voir de fraudes.

Tout vérificateur placé devant une comptabilité utilisant un ordinateur devra adopter sa méthode de travail. Une question fondamentale est posée : peut-il ou doit-il utiliser l'ordinateur pour son contrôle ? Un double problème se pose alors :

- Un problème législatif : le droit de communication et de contrôle porte sur des documents dont la tenue est prescrite par le Code de Commerce. Toutefois la présentation effectuée sous cette forme n'est pas forcément antérieure à la vérification. Au surplus, antérieurement au 1.1.1982, aucun moyen légal n'obligeant l'entreprise à mettre son ordinateur à la disposition du vérificateur. Si ces moyens existent maintenant leur mise en oeuvre n'ira pas sans réticence de la part des entreprises.

Le vérificateur n'a pas non plus le droit d'emporter des supports de l'information (bandes magnétiques, disques...) qu'il souhaiterait faire traiter par un ordinateur de la D.G.I. avec des programmes généraux de contrôle. Toutefois aucun texte ne s'oppose à ce qu'il en prenne copie. La nouvelle brigade spécialisée envisage d'utiliser un ordinateur portable qui lui permettrait de saisir l'information dans l'entreprise vérifiée et de l'exploiter sur des ordinateurs de l'Administration.

- Un problème technique : si le vérificateur doit avoir un minimum de connaissances informatiques, il n'est pas, pour l'instant capable d'utiliser correctement un ordinateur, sauf à faire appel à une assistance technique de haut niveau.

En raison de ces nombreux problèmes légaux et techniques il est probable que la vérification sans assistance de l'ordinateur restera pour longtemps encore la méthode la plus courante. Cependant, il est indispensable, tout en restant autour de l'ordinateur, de ne jamais l'ignorer et d'y adapter la méthode de vérification.

Dès lors le vérificateur ne peut plus se limiter à l'exploitation des documents qui lui sont remis. En revanche il doit utiliser pleinement les possibilités qui lui offrent les textes puisque l'exercice du contrôle doit comporter droit d'accès à la documentation relative aux analyses, à la programmation et à l'exécution des traitements.

Un certain nombre de réflexes nouveaux doivent conduire à poser des questions efficaces, techniques. L'Inspecteur fera ainsi preuve de compétence et évitera d'être "manipulé" par les techniciens de l'entreprise qui ont parfois tendance à avancer des arguments techniques pour se soustraire à leurs obligations.

Il ne peut être envisagé de donner ici une description complète de ces réflexes mais plutôt de tracer des directions de recherche :

1) S'informer sur la conception générale du système : type d'équipement, personnel, organisation du département informatique, ses liens avec les autres services, sécurité des installations.

2) Demander le dossier d'analyse qui doit comprendre :

- une description fonctionnelle des traitements
- un organigramme général
- une description organique des traitements.

Le dossier d'analyse décrit les entrées et les sorties et les contrôles effectués à cette occasion, donne la liste et la composition des fichiers, la durée de leur stockage etc...

3) Consulter les dossiers d'exploitation qui donne

- une description de l'objet de chaque programme
- un organigramme d'enchaînement
- l'indication des différentes phases d'opérations à mettre en oeuvre
- la désignation des fichiers à utiliser et à protéger
- la liste des messages émis lors de l'exécution du traitement
- les fichiers et états de sortie.

4) Obtenir la liste de toutes les bandes contenues dans la bandothèques ainsi que l'historique de toutes les bandes et fichiers.

5) Demander à avoir accès à la "boîte noire" de l'ordinateur qui décrit les traitements effectués à tout moment (mais peut-on y avoir accès ?).

Le chapitre qui suit a pour objectif de donner quelques contrôles que le vérificateur pourra effectuer.