(1)

Sous la présidence de Maître Yves REPIQUET,

bâtonnier de l'Ordre

La justice à l'épreuve de la preuve immatérielle

Débats animés par Michel ARMAND-PREVOST et Thomas CASSUTO

Mercredi 21 novembre 2007

Maison du Barreau à Paris

❖ ❖ ❖

(1) Institut PRESAJE : Prospective, recherches et études sociétales appliquées à la justice et à l'économie.

S O M M A I R E

Me Michel ARMAND-PREVOST.- Monsieur le Bâtonnier, vous avez la parole.

Yves REPIQUET.- Le sujet qui a été choisi : *"La justice à l'épreuve de la preuve immatérielle"* est un sujet très important, qui s'inscrit dans ce qu'a toujours recherché PRESAJE, c'est-à-dire d'être non seulement dans la prospective, mais aussi dans la réalité quotidienne.

La Preuve et l'Immatériel, voilà deux notions qui paraissent non pas antinomiques, mais bien étrangères l'une à l'autre. Dans le procès, la preuve doit être le terrain de la matérialité, du concret, du réel, du palpable, de l'objectif. L'immatériel, l'évanescent, ce que l'on n'arrive pas justement à palper, à capter, à percevoir, à mettre sur un support accessible facilement à l'homme semble devoir rester étranger au droit de la preuve.

Pourtant, juges, magistrats et avocats, nous pratiquons tous depuis des décennies la preuve immatérielle. Et cela depuis que l'usage de la photocopieuse est partagé par le plus grand nombre pour ne pas dire par tous, et peut-être même depuis plus longtemps encore. En effet, dans le procès civil, combien de fois entend-on un juge ou un avocat demander que soit produite la pièce originale ? Il est très rare que le cas se présente, sans pour autant que la preuve perde en "qualité", en force probante. C'est qu'une preuve s'apprécie rarement *ex-nihilo*, elle s'inscrit dans un ensemble d'un faisceau de preuves, d'autres preuves, d'autres informations et de pratiques qui concourent à sa crédibilité, c'est-à-dire sa force probante.

Par le truchement de la photocopie, qui devient le mode de circulation d'une information probatoire, dont l'original est conservé par l'une des parties, voire un tiers, chacun des acteurs du procès accorde sa confiance à l'information probatoire dont elle est le vecteur. Finalement, la preuve a toujours reposé sur la confiance, confiance dans le support qui la renferme, mais aussi dans la personne, c'est-à-dire le professionnel qui l'utilise. Et déjà, on le comprend, l'immatériel s'immisce dans le droit de la preuve. On pourrait même dire qu'il le sous-tend.

L'écrit moderne étant immatériel, déjà les procès commerciaux sont envahis d'e-mails que chacun s'oppose mais que personne ne dénie, de communications entre avocats et juridictions. Personne ne dénie la force probante de ce support. Ce n'est pas le moindre des paradoxes de constater que lorsque l'on produit à des fins probatoires un e-mail, un courrier électronique. Quant au pénal, la preuve est libre.

Un décret a été publié à la suite de la loi du 5 mars 2007, qui permettra désormais aux avocats d'avoir un accès direct, par le biais de l'Internet, aux dossiers en matière pénale. Je considère pour ma part que cette évolution relève de la révolution et que c'est enfin le moyen le plus adapté, le plus sûr de garantir l'exercice des droits de la défense dans une information judiciaire. Il y avait quelque chose d'anormal, à l'époque où nous vivons, à ce qu'il faille qu'un cabinet d'avocat envoie l'un des siens frapper à la porte d'un juge d'instruction pour avoir accès au dossier, le consulter, commander une copie. Il est normal que, dans un exercice complet des droits de la défense, l'avocat puisse avoir un accès direct et en temps réel, pour pouvoir exercer véritablement les droits de la défense.

Le fait que des avocats puissent désormais indiquer leur adresse électronique aux magistrats instructeurs fera qu'ils recevront des notifications des actes de la procédure et, singulièrement, l'acte final qui sera l'ordonnance de règlement. Ce qui permet un meilleur exercice des droits de la défense, car la jurisprudence a tranché non pas pour la date de

réception de la notification de l'acte mais pour son émission, si bien que, dans des délais assez courts, l'avocat perdait un nombre de jours importants pour l'exercice des droits de la défense. Nous sommes donc véritablement au cœur d'un sujet plus général qui touche à l'ensemble de nos procédures.

Finalement, ce que preuves matérielle et immatérielle ont en en commun, c'est bien la confiance. Quelle confiance accorder à la preuve immatérielle ? Comment accorder sa confiance à une preuve immatérielle ? A quel acteur du processus de réalisation d'une preuve matérielle accorder ou ne pas accorder sa confiance ? C'est aujourd'hui le nouveau paradigme à inventer.

Dans cette recherche, deux considérations peuvent, me semble-t-il, nous servir de guide :

- Ne cherchons pas à vouloir doter la preuve immatérielle de ce que la preuve matérielle n'a jamais eu : l'infaillibilité,
- N'oublions pas que ce qui n'est pas contesté n'a pas à être prouvé.

Je vous remercie.

1ère table ronde : Le juge civil face à la preuve immatérielle, sous la présidence de Me Michel ARMAND-PREVOST

M. le Président.- Je vous présente d'abord les intervenants :

- Me Christiane FERAL-SCHUHL, avocat à la cour, ancien membre du Conseil de l'ordre des avocats de Paris,
- Me Maurice LOTTE, huissier de justice à Paris,
- M. Emmanuel BINOCHE, premier vice-président au tribunal de grande instance de Paris, chargé du service des expertises,
- M. Stéphane LIPSKI, expert en informatique et en comptabilité, agréé par la Cour de cassation, président de la Compagnie Nationale des Experts de Justice en Informatique et Techniques Associées (CNEJITA).

Cette table ronde comportera trois temps :

- présentation des textes,
- difficultés présentes,
- les perspectives.

1. Présentation des textes sur la preuve électronique

Les dispositions du Code civil sur l'écrit électronique et la preuve numérique ont été introduites dans ce Code par trois textes successifs :

- la loi du 13 mars 2000,
- la loi du 21 juin 2004,
- l'ordonnance du 16 juin 2005.

Je veux simplement vous montrer la construction des dispositions du Code.

Ces dispositions figurent dans le troisième Livre, Titre III, intitulé « des contrats ou des obligations conventionnelles en général ». Les premières dispositions dans l'ordre de la numérotation du Code sont, au chapitre II, les conditions essentielles pour la validité des conventions. L'article 1108-1 énonce : *"Lorsqu'un écrit est exigé pour la validité d'un acte juridique, il peut être établi ou conservé sous forme électronique."* Dans le chapitre VI « de la preuve des obligations et de celle du paiement » figure une section 1 « de la preuve littérale », dans laquelle on trouvera des dispositions générales. La définition de ce que peut être une preuve littérale montre que l'on introduit la notion d'écrit électronique, puisque l'article énonce : *"La preuve littérale ou preuve par l'écrit résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leur modalité de transmission."* Enfin, l'article 1316-1 énonce le principe même : *"L'écrit sous forme électronique est admis en preuve au même titre que*

l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité."

Un chapitre est ensuite complètement consacré aux contrats sous forme électronique, avec les échanges d'information. Ces dispositions ont été introduites par l'ordonnance du 16 juin 2005. Une deuxième section concerne les conditions de conclusion d'un contrat sous forme électronique, une troisième est relative à l'envoi ou à la remise d'un écrit par voie électronique, la dernière a trait à certaines exigences de forme.

Mme Christiane FERAL-SCHUHL, en tant qu'avocat, qu'est-ce que ces textes ont changé dans la construction d'un dossier ?

Christiane FERAL-SCHUHL.- Rien parce que, aujourd'hui, culturellement et spontanément, on produit tous un certain nombre de documents dématérialisés. Chacun de ces textes a progressivement élargi le champ d'admission de la preuve. On pouvait bien sûr, avant la loi du 13 mars 2000, produire des documents, des éléments de preuve. Il nous arrivait de produire des télécopies. L'admission de la preuve était circonscrite à ce que l'on appelle l'écrit *ad probationem*, la production d'un écrit pour établir la réalité d'un fait.

La loi du 13 mars 2000 a favorisé, élargi, précisé dans quelles conditions on peut effectivement, pour établir un fait, produire ces éléments. Il y a eu une avancée notable avec la deuxième loi dont vous avez parlé, celle de 2004, qui a permis de se concentrer sur l'acte juridique. Dans le domaine de l'acte juridique, la signature produira des effets, des conséquences juridiques. Ce sera par exemple la production d'un bail.

En précisant les conditions d'admission de cette preuve, un élargissement considérable a été apporté. On va rentrer dans cette notion d'équivalence de l'écrit électronique et de l'écrit original traditionnel papier. Une avancée encore plus forte avec l'ordonnance du 16 juin 2005 me permettra, même dans les cas où un formalisme est imposé, en particulier au Code de la consommation, de produire des éléments que je ne pouvais pas produire auparavant.

Pour ne donner qu'un exemple, l'accusé de réception pourra être remplacé par un accusé électronique. Je pourrai fournir un formulaire détachable, donc un formulaire électronique alors qu'auparavant je devais justifier de l'existence du double ou du triple du formulaire. On voit donc des pans entiers d'un formalisme qui était là pour protéger, pour établir la preuve qui, petit à petit, reculent et ouvrent un champ d'admission de la preuve. Par conséquent, dans la construction de mon dossier, j'ai une facilité de production de la preuve et de l'admission de la dématérialisation dans les preuves que je produis.

On ne peut pas déconnecter la problématique de la preuve de la signature électronique qui est le corollaire de la preuve, mais également de l'archivage. Il ne faut pas perdre de vue qu'au moment où je produirai mon élément de preuve, ce sera forcément postérieurement au moment où je me suis servie de l'écrit électronique, après vous avoir envoyé un e-mail. Le jour où je voudrais établir que j'étais bien ici à la date du 21 novembre pour cette conférence, je restituerais des éléments qui, eux-mêmes, auront été archivés et qui devront avoir respecté un formalisme.

M. le Président.- Je me tourne maintenant vers l'expert : l'écrit électronique a-t-il perturbé ou non le déroulement d'une expertise judiciaire ?

Stéphane LIPSKI.- Monsieur le président, je répondrai comme Me FERAL-SCHUHL : cela l'a facilité et l'a grandement perturbé. Cela l'a facilité, d'une part parce que la communication des informations se fait de manière beaucoup plus simple. Aujourd'hui, en expertise judiciaire, souvent les informations ne sont plus transmises sous forme papier mais sous forme électronique et de mail, pour une raison très simple : Souvent, on a de tels volumes d'informations que ce serait non traitable sur un support papier. L'expertise judiciaire se caractérise souvent aujourd'hui par l'envoi de mails d'avocats à experts, avec une information en fait plus facilement contradictoire parce que l'on peut normalement s'assurer que tout le monde a bien reçu la même information en même temps, avec un certain nombre de perturbations.

Le premier point est le volume des informations. Aujourd'hui, en expertise judiciaire, on est envahi par l'information. Comme le disent les informaticiens, trop d'information tue l'information. La communication d'informations est aisée avec l'informatique, en particulier avec les mails. On peut donc être abreuvé d'une grande quantité d'informations.

De nombreuses opérations d'expertise reposent sur des informations qui étaient auparavant présentées sous forme d'écrit, en dix, cinquante ou cent pages, et qui sont aujourd'hui présentées sous forme de mail, représentant un, deux ou trois classeurs. Nous avons énormément d'informations, avec une autre difficulté importante : le problème de la datation. Il existe naturellement des problèmes de difficulté de datation des écrits papier, mais, lorsque que l'on parle d'écrit électronique, la datation est toujours sujette à caution. On peut toujours vous dire que la date qui apparaît sur cet écrit électronique n'est pas la bonne date parce que, on peut toujours modifier une date. Je peux très bien, dans mon ordinateur, changer la date, transmettre une information en faisant croire que c'est une autre date. Cela arrive effectivement très rarement et, en l'occurrence, le problème ne se pose généralement pas, mais l'expert doit en tenir compte.

L'autre point est la conduite de la mission. Peut-on se contenter de dire que toutes les informations électroniques que l'on reçoit sont des informations que l'on considérera comme fiables ou faut-il mettre en place un système avec une vraie sécurité de ses communications ? Une société notamment constituée d'experts judiciaires, avec un système appelé Opalex, a essayé de développer un système qui permettait d'avoir un écrit électronique, des messages et une conservation contradictoire qui soient d'une certaine manière chiffrés. Ceci signifie naturellement que cela complexifie largement l'expertise judiciaire et, en l'occurrence, c'est peu utilisé puisque l'on trouve déjà l'expertise judiciaire suffisamment complexe en elle-même.

Il y a donc des éléments de facilitation, mais aussi beaucoup de difficultés.

Un dernier point concerne les litiges qui peuvent intervenir dans ce domaine. Jusqu'à présent il y en a peu, mais parler du système de signature électronique signifie que nous sommes sur des systèmes techniquement très évolués et assez complexes à vérifier.

Le principe du chiffrement habituel signifie que j'ai un texte, je vais le coder avec une clé de codification, je vais le transmettre à un tiers qui utilisera cette même clé de codification pour trouver l'origine du texte. Ce principe n'est pas suffisamment sûr. Aujourd'hui, les systèmes sécurisés sont des systèmes dits à clé asymétrique. Je vais utiliser une clé, qui est ma clé privée, et j'envoie à un tiers qui utilise une clé dite publique qui n'est pas la même que la mienne, mais la procédure de chiffrement et de déchiffrements fait qu'il peut arriver à relire mon texte.

Vous imaginez que ces procédures sont complexes, assez mathématiques. Si l'on part sur des expertises sur ces systèmes qui peuvent être mis en cause, le résultat peut être assez complexe. Le problème ne s'est pas encore vraiment posé pour l'instant, mais je fais de la prospective sur l'avenir.

M. le Président.- Merci. Monsieur l'huissier, est-ce que ces textes ont modifié l'exercice de votre métier tant dans votre activité de recouvrement de créances que dans l'exécution des décisions de justice ?

Me Maurice LOTTE.- En ma qualité d'huissier de justice et donc d'officier public et ministériel, rédacteur d'actes authentiques, la problématique de la signature et des conditions de conservation d'un acte d'huissier de justice sur support numérique prend toute son acuité. A votre question, la réponse est aujourd'hui clairement négative.

Il faut toujours garder à l'esprit que, dans son activité et dans les actes dont il est rédacteur, l'huissier de justice dispose d'une énorme variété. Ces actes peuvent être classifiés en différentes catégories :

- les actes à caractère informatif (une assignation, une signification de décision),
- des actes à caractère exécutoire (un acte d'exécution, une mesure de saisie, une mesure d'expulsion),
- et enfin des actes qui sont des rapports de constatations ou des constats, qui feront ensuite l'objet de communications et transmissions à l'égard des tiers.

Les textes que nous avons évoqués tout à l'heure n'ont qu'une incidence extrêmement réduite sur le décret de février 1956 qui régit le statut des huissiers de justice dans leur rôle de rédacteurs d'actes authentiques. En effet, ils ne se concentrent exclusivement que sur les conditions de conservation sur support numérique et accessoirement, à terme, par les outils gérés par la Chambre nationale des huissiers de justice dans la gestion et dans la notion de ce que l'on appellera ultérieurement un minutier central. Ce minutier central, qui a vocation à être détenu sous forme de coffre-fort électronique par la Chambre nationale des huissiers de justice, permettra à celle-ci de conserver l'intégralité et l'intégrité du contenu de tous les actes d'huissiers de justice signifiés et rédigés en France, avec accès restreint aux seuls huissiers de justice à partir de leur certificat et de leur signature numérique auxquels sont adossées la clé publique et la clé privée dont M. LIPSKI a fait état tout à l'heure.

Dans la pratique, dans les mesures de recouvrement de créances et plus précisément d'exécution des décisions de justice, pourquoi ces textes n'ont pratiquement pas l'usage de s'appliquer, et ce pour plusieurs raisons. D'abord et avant tout parce qu'un acte d'huissier de justice répond à deux conditions. La première, celle qui est reprise dans le décret de 1956, est l'obligation d'établissement des actes en doubles originaux. Ces deux originaux peuvent être conservés et transmis ultérieurement dans le cadre de l'instance sur support numérique dans les conditions de transmission qui vous ont été évoquées. En revanche, ne perdons jamais de vue qu'un acte d'huissier de justice, pour conserver sa validité, doit d'abord et avant tout être signifié. A l'égard du tiers destinataire de l'acte d'huissier, cet acte d'assignation ne pourra bien évidemment en aucune manière avoir un support numérique à l'égard du destinataire. Il faudra qu'il y ait un réel contact, un réel face à face, et la copie de cette assignation à l'égard de ce tiers destinataire a pour lui valeur d'original. Il ne peut aujourd'hui y avoir d'autre support qu'un seul et unique support papier. En effet, cet acte d'huissier de justice, qu'il soit un acte informatif ou un acte d'exécution, n'a de valeur que s'il est signifié et valablement signifié. Aujourd'hui, les règles de signification des actes, quelles

qu'en soient les modalités (remise à sa personne ou remise par défaut à l'étude de l'huissier ou accessoirement une signification à parquet), ne peut avoir qu'un support exclusivement papier.

L'autre aspect où les huissiers de justice ont eu une certaine avancée se situe dans le cadre de "l'exécution", dans une action spécifique de recouvrement de créance, aussi appelée le recouvrement amiable ou le recouvrement pré-contentieux. Dans ce cadre, dès lors qu'il n'y a pas titre exécutoire soumis à exécution par huissier de justice, l'ensemble des "actes" (relances, lettres comminatoires ou interventions spécifiques à l'égard d'un débiteur quel qu'il soit pour une créance quelle qu'elle soit), l'intégralité des échanges entre un huissier de justice et son donneur d'ordre seront exclusivement numériques. Le format en est très simple : le donneur transmettra à un huissier un tableau généralement sous format Excel comprenant un certain nombre de données informatives qui seront reprises par l'huissier de justice soit sous forme de publipostage, soit sous forme d'interface spécifique au logiciel de traitement et de gestion de son étude. Cela lui permettra de créer, mais hélas exclusivement sous format papier, certains courriers (relances, mises en demeure, interventions, lettres comminatoires), et ce de quelque nature qu'ils soient.

Voilà rapidement, monsieur le président, les conséquences de la conservation des actes d'huissier au regard des textes qui nous occupent aujourd'hui.

M. le Président.- Je vais maintenant poser une question au juge en revenant sur l'article 1316-2 du Code civil. Cet article prévoit que le juge règle les conflits de preuve littérale en déterminant par tous moyens le titre le plus vraisemblable, quel qu'en soit le support. Au regard de ce texte, y a-t-il d'ores et déjà eu beaucoup de conflits dans lesquels était en cause une preuve électronique, monsieur le président ?

Emmanuel BINOCHE.- A vrai dire, pour répondre à cette question, je pense à ce qui vient d'être dit : on a toujours plus ou moins, suivant le degré de dématérialisation des actes, une référence plus ou moins grande à l'original de l'acte.

Mais, si l'on répond directement à la question, on s'aperçoit effectivement qu'il y a plusieurs raisons pour lesquelles il y a peu d'occasions de conflit. D'abord parce que, dans la réalité des choses, il est, me semble-t-il, relativement rare de voir confrontés deux actes totalement contradictoires, sauf si l'on se situe peut-être dans une phase précontractuelle où l'on peut avoir différents projets confrontés et qui représentent l'évolution des discussions. Mais, selon mon expérience, une fois l'accord ou le contrat passé, il est rare de voir un véritable conflit de preuve littérale au sens de l'article 1316-2.

Je voudrais tout de même attirer votre attention sur 2 formules rédactionnelles essentielles :

- *"A défaut de convention valable entre les parties"* signifie que, notamment quand l'on pense à la matière commerciale, il y a possibilité de prévoir *a priori* la manière dont on peut résoudre ce genre de conflit,

- *"A défaut, il est question pour le juge de déterminer par tous moyens le titre le plus vraisemblable*" : cela laisse au juge une liberté grande et importante. Selon moi, cela caractérise la tendance du législateur dans ce domaine de la preuve immatérielle en particulier et dans le domaine de l'immatériel en général.

J'ai récemment rencontré une difficulté posée par la notification prévue par la loi du 21 juin 2004 pour la confiance dans l'économie numérique, notification préalable à une

demande qui peut être faite en référé d'avoir à supprimer des contenus illicites ou en tout cas de mettre fin à leur accès. Sa forme n'est pas précisée. En particulier, il n'est pas précisé qu'il faille recommander la notification ni qu'il faille une demande d'avis de réception. C'est par un courriel qu'avait été faite cette notification, de manière d'ailleurs assez incomplète au niveau de l'articulation des éléments de fait et de droit. Déjà, en soi, était contestée la réception de ces courriels qui étaient au nombre de deux. Toutefois, celui qui faisait état de cette notification n'avait pas pris la précaution de demander ce que l'on appelle de manière traditionnelle actuellement en matière de courriel un "avis de réception", qui d'ailleurs n'a pas la valeur d'un véritable avis de réception au sens où on l'entend quand on est sur un support écrit. Il n'avait même pas la possibilité d'établir que ce message avait été lu sur l'ordinateur de son correspondant. Celui-ci s'est abrité sur le fait qu'il n'avait pas reçu, en tout cas qu'il n'y avait pas la preuve qu'il ait reçu cette notification. Voilà un exemple de conflit qui a eu pour conséquence de ne prendre en compte que l'acte introduisant l'instance.

Il est vrai que j'ai aussi plutôt eu une expérience de litiges commerciaux où la preuve est libre et où, depuis très longtemps, les parties acceptent de part et d'autre les télécopies et les photocopies sans grande difficulté. Dans ce contentieux, je n'ai pas non plus rencontré de conflit véritable. Il faut là rendre justice la jurisprudence de la Chambre commerciale de la Cour de cassation, qui, dès le 2 décembre 1997, avait admis cette preuve par télécopie, sous certaines conditions : la possibilité de garantir l'intégrité du document et son imputabilité à celui à qui on l'opposait.

La référence que l'on peut faire pour l'appréciation de ce risque de conflit est la différence en matière de preuve entre la matière commerciale et la matière purement civile.

Un principe est également monté en puissance ces dernières années : le principe de loyauté non seulement dans le comportement précontractuel, voire contractuel, mais aussi dans le comportement procédural. C'est un frein qui me paraît assez efficace à des objections qui seraient opposées non seulement de mauvaise foi, mais même de manière déloyale. Si bien que cela explique sans doute que l'on rencontre peu de conflits de preuve littérale. Je voudrais ajouter que l'on irait presque dans la procédure expertale française à constater les excès que l'on peut relever dans la procédure de *discovery* aux Etats-Unis. Quel que soit le mode de communication que l'on utilise pour produire des preuves, il me semble qu'il faut respecter des règles de base que tous les avocats connaissent, à savoir la numérotation des pièces. La convention du 4 mai 2006 sur l'expertise civile avait prévu en particulier la numérotation en continu pour que l'expert puisse s'y retrouver. Je crois que des horodatages, quel que soit le support, sont absolument indispensables, ainsi que des numérotations de pièces. C'est le minimum pour que l'expert s'y retrouve, et aussi que l'on puisse veiller au respect du contradictoire, car le contradictoire n'est pas éludé, loin s'en faut, par le recours à la transmission électronique.

2. Difficultés présentes

M. le Président. - Nous allons maintenant essayer de voir quelques difficultés concrètes. Tout d'abord, cette fiabilité nécessaire : la mise en place d'une signature électronique fiable et les obligations des prestataires de service de certification. Monsieur Lipski, voulez-vous bien reprendre la parole sur ce thème.

Stéphane LIPSKI.- Pour répondre et compléter, je suis naturellement d'accord avec ce que disait M. BINOCHE. La seule difficulté aujourd'hui est le volume des

informations et pas tellement la numérotation. Lorsque vous recevez des pièces par centaines ou par milliers, il y a un vrai problème de volume que l'on rencontrait beaucoup moins il y a dix ou vingt ans.

Je vous donne un exemple de mise en place d'une signature électronique fiable avec toute la complexité qu'il y a derrière en prenant ma double casquette d'expert en informatique et d'expert en comptabilité, celui de la Compagnie nationale des commissaires aux comptes qui a mis ceci en place il y a deux ans. Nous avions une difficulté dans l'émission de nos rapports généraux en tant que commissaires aux comptes. Cela peut paraître étonnant, mais certains cabinets et commissaires aux comptes d'OPCVM devaient émettre leur rapport pour un millier d'OPCVM. Ces rapports étaient trimestriels et devaient être remis de manière urgente parce que les OPCVM ont des obligations de publication et d'information rapides.

Emettre mille rapports à signer et transmettre très rapidement posait de vrais problèmes pour un cabinet. Une solution pratique a été mise en place avec l'écrit électronique, signature électronique fiable. Qui dit signature électronique fiable signifie, pour répondre aux différentes prescriptions légales, qu'il faut tout d'abord une autorité de certification, c'est-à-dire que l'on définit la politique de certification. Une politique de certification signifie que l'on utilise des certificats qui peuvent être de trois sortes. Il y a plusieurs classes :

- La première classe signifie qu'il y a uniquement une communication par mail. On ne connaît donc l'identité de la personne à qui l'on va délivrer le certificat que par une communication mail. C'est naturellement un niveau de sécurité faible ;

- La classe 2 consiste à communiquer les informations d'identité par voie postale. C'est le système que l'on a par exemple avec les cartes bancaires et les numéros que l'on reçoit ;

- La classe 3, qui est la plus sûre, consiste à avoir une communication en face à face. On ne communique le certificat qu'à une personne qui vient se présenter et qui présente son identité.

Une autorité de certification, en l'occurrence la Compagnie nationale des commissaires aux comptes, a d'ailleurs défini des autorités locales de certification puisque des commissaires aux comptes sont présents sur toute la France. Cela signifie que l'on n'obligera pas un commissaire aux comptes à venir à la compagnie à Paris. Il ira à la compagnie régionale de commissaires aux comptes dont il dépend dans sa région pour se présenter et obtenir le certificat.

Il faut par ailleurs une autorité d'enregistrement : c'est la personne qui vérifie que celui qui demande un certificat est bien celui qu'il prétend être. Non seulement on va demander un certificat, mais on ne donnera un certificat qu'à une personne dont on vérifiera qu'elle est bien commissaire aux comptes et qu'elle figure bien sur la liste. Il faut ensuite des opérateurs de certification. Il s'agit de sociétés spécialisées qui réalisent techniquement, diffusent techniquement le certificat au cas particulier. La Compagnie des commissaires aux comptes s'est adressée à la société Certplus. Il y a peu d'opérateurs de certifications. Nous avons lancé, comme nous le faisons d'habitude, un appel d'offres.

Un lecteur de carte à puce est communiqué aux commissaires aux comptes avec une carte à puce nominative du genre carte bleue. Ce n'est valable que trois ans, toujours pour accentuer la sécurité. Tous les trois ans, le commissaire aux comptes doit changer sa carte. Il faut naturellement un logiciel adapté qui réalise la cryptologie dont j'ai parlé sur la clé

asymétrique. C'est valable pour n'importe quel client dans le cadre d'une communication d'un rapport général, mais, il faut le reconnaître, cela fonctionne essentiellement avec les OPCVM. Il faut leur communiquer un logiciel qui sera le logiciel qui contiendra la clé publique que chaque société utilisera pour déchiffrer le rapport général qui sera communiqué.

Cela fonctionne bien. Ce n'est pas encore complètement diffusé à tous les clients et toutes les sociétés que les commissariats aux comptes peuvent avoir, mais je pense que ce système présente plus de garanties que l'écrit. Quand j'émets un rapport que je vais transmettre, la sécurité quant à la date est relative parce que je peux mettre n'importe quelle date dans mon écrit. Avec une communication sous cette forme, on peut toujours imaginer que le commissaire aux comptes est allé changer la date dans son système informatique, bien que ce soit peu probable. Les systèmes électroniques présentent aujourd'hui un degré de fiabilité dont on peut considérer que, souvent, si l'on utilise des outils de ce type, avec une forte classe de sécurité, ils sont pratiquement aussi sûrs que l'écrit. Il ne faut pas non plus présenter trop de défiance à l'égard de l'informatique et le rendre inopérant. La Compagnie représente un bon exemple en la matière.

M. le Président.- Maître FERAL-SCHUHL, comment démontrer que les garanties d'authentification et d'intégrité ont bien été mises en œuvre ?

Christiane FERAL-SCHUHL.- Je constate, monsieur le président, que l'on demande plus finalement à l'écrit électronique qu'à l'écrit papier parce que, avec la production d'écrit papier, on vérifiait les signatures. Votre question conduit à savoir dans quels cas, finalement, ces garanties d'authentification et d'intégrité sont acquises. Elles sont acquises par la signature électronique avancée qui est le choix qui a été fait par le législateur, et la loi du 13 mars 2000 a entériné ces fonctions d'intégrité et d'authentification, instaurant pour la signature électronique répondant à ces prescriptions une présomption de fiabilité. Cette présomption supposera déjà qu'il y ait une contestation. A partir du moment où j'établis que je me suis conformée au dispositif prévu par loi, je suis présumée offrir toutes ces garanties d'authentification et d'intégrité.

Quelles sont-elles ces garanties ? La présomption de fiabilité jouera en faveur des personnes qui auront recours à des produits correspondants soit à des normes mentionnées dans une liste publiée au JO des communautés européennes, soit à des tiers prestataires de services de certification. La création de la signature électronique comporte plusieurs étapes puisqu'il faudra recourir à un dispositif de création de signature qui doit être sécurisé. Il y aura un dispositif de vérification de la création de la signature électronique. Il y aura le dispositif de sécurité de la vérification, le prestataire de certification qui émettra le certificat. C'est un peu le procédé qui vient d'être décrit par M. LIPSKI.

Ces différentes phases supposent des étapes de certification. A partir du moment où j'utilise un certificat, cette garantie existera. Aujourd'hui, si vous télépayez vos impôts, l'émission d'un certificat est là pour certifier d'abord que le signataire est bien celui qui émet le message et que le message a bien été adressé, que le contenu est le même entre le moment où le message est envoyé et le moment où il est reçu.

Une notion apparaît peut-être dans cette discussion : une distinction est en train de s'opérer entre l'intégrité technique et l'intégrité juridique du document. L'intégrité technique conduira à considérer que l'intégrité n'est pas respectée à partir du moment par exemple où un bit disparaît lorsque l'on comparera les deux documents électroniques en même temps. Des procédés techniques permettront de constater le différentiel et donc l'atteinte à l'intégrité. Mais aussi, la notion d'intégrité juridique fera que l'on peut ne pas avoir porté atteinte à l'intégrité

juridique du document parce qu'on a modifié un accent. L'intégrité technique identifiera tout de suite qu'en supprimant un accent on a supprimé un caractère technique qui, du coup, posera la question de l'identité du document. Comme la garantie technique et l'identité technique résultent du choix de la signature électronique, il va de soi, pour garantir et préserver toutes garanties d'authentification et d'intégrité, qu'il faudra conserver tous les éléments ayant permis de conduire à l'émission de ce message.

Un parallèle est sans doute à faire ici avec le contrôle en matière de comptabilité informatisée. En matière fiscale, lorsque l'on procède à un contrôle des comptabilités informatisées, il est demandé de conserver tous les éléments qui conduisent à justifier des résultats produits à titre de preuve. Les comptabilités informatisées ont finalement été les premiers éléments dématérialisés à entrer dans la vie quotidienne des entreprises. Les différentes étapes qui ont conduit à l'émission de ces éléments donnent lieu à la conservation de ces éléments. Je n'ai jamais été confrontée à la démonstration à faire de ces garanties d'authentification et d'intégrité parce que lorsque, dans un dossier d'avocat, on produit un document, une présomption très forte existe dans la production de ce document. On peut imaginer qu'il y aura à terme des contestations, et la preuve pourra se faire sans doute par la démonstration que les empreintes électroniques ont bien été conservées pour rétablir l'historique de la création du document électronique au moyen de la signature électronique.

M. le Président.- Dans la pratique, peut-on avoir recours utilement à des signatures électroniques qui ne bénéficient pas de la présomption légale de fiabilité ?

Christiane FERAL-SCHUHL.- Les solutions techniques et les signatures électroniques qui ne remplissent pas les critères imposés par les textes existent depuis longtemps et offrent depuis longtemps des garanties d'authentification. Prenez l'authentification des paiements. Les cartes bancaires existent depuis longtemps et les tribunaux ont déjà eu à se pencher sur ces questions et à considérer que, à partir du moment où il y avait suffisamment d'éléments probants pour établir la réalité de l'opération, il n'y avait pas de difficultés.

La signature électronique ordinaire existe donc. Elle est d'ailleurs prévue par la directive européenne, et certains pays ont opté pour la mise en place d'une signature ordinaire par opposition à la signature électronique avancée qui est le choix de la France, qui a prévu tous ces systèmes de contrôles renforcés pour créer cette présomption de fiabilité au moyen des garanties d'intégrité et d'authentification. Les exemples, nous les avons déjà. Il est possible d'y recourir, mais, surtout, il existe depuis longtemps les conventions de preuves. Il est tout à fait possible, dans le cadre d'un accord bipartite, de décider que l'on se contentera de signatures ordinaires ou que telles productions d'éléments vaudront preuve acceptée par l'autre partie. Les conventions de preuve trouvent des applications de plus en plus généralisées pour une raison simple :

- la signature électronique avancée est complexe,
- elle est un frein à l'utilisation de manière générale aux signatures,
- on entre dans ces processus de plus en plus facilement et elles font autorité.

Une décision a d'ailleurs été rendue, qui a tranché sur la question de la validité de ces conventions de preuve. Donc, il est parfaitement possible de recourir à des systèmes moins catégoriques, moins précis que ceux énoncés par les textes.

M. le Président.- Merci. Maître Lotte, quel est le point de vue de l'huissier sur cette question ?

Maurice LOTTE.- Il est complètement proche de celui de Me Christiane FERAL-SCHUHL. Pour rappel, l'utilisation de la signature électronique, du point de vue de l'huissier n'a vocation qu'à assurer la certification du signataire, l'intégrité du document et le fait que l'on ne puisse pas le modifier dans un seul et unique souci de conservation. Maintenant, sur la fiabilité ou l'éventuelle dégradation des données techniques propres à déterminer la signature électronique, il existe plusieurs degrés. On sait, au niveau de la signature électronique, que plusieurs degrés de fiabilité et degrés d'identification de la qualité du signataire existent. L'huissier de justice utilisera dans ses rapports professionnels la signature électronique de son point de vue dans un seul et unique cas : la transmission des pièces dont il a, par nature, la conservation et dont il assume la responsabilité. Ce sont ces actes, ce sont ces minutes qui peuvent être transmises par voie dématérialisée.

Maintenant, dans l'autre sens de l'échange, les huissiers de justice offrent aujourd'hui certains services à l'égard de sociétés, de tiers, de personnes physiques quelles qu'elles soient. Les plateformes des offices d'huissiers de justice sont aujourd'hui de plus en plus dématérialisées. Il est possible d'assurer un paiement en ligne. Il est possible, pour un client, d'avoir accès aux données personnelles d'un ou plusieurs des dossiers qui sont en gestion dans l'office. Il est également possible à l'huissier de justice d'enregistrer sur cette plateforme dématérialisée certains dépôts, des règlements de jeux concours, des dessins et modèles ou certains éléments qui viendront en annexe ou en complément d'un rapport de constatation ou d'un acte judiciaire ou extrajudiciaire dont il aura eu la charge de la signification. Y aura-t-il, à l'égard de l'huissier, un contrôle réel de la part de l'expéditeur ou de la personne qui lui adresse ces documents ? Faudra-t-il de s'assurer s'il y a eu de sa part l'usage d'une signature électronique et d'une vérification du certificat ?

Aujourd'hui, soyons clairs, la réponse est négative. L'absolue majorité des documents et des informations qui sont communiqués par les tiers (entreprises, avocats, personnes physiques, particuliers) à l'intention de l'huissier de justice, notamment au travers des mails et des données dématérialisées sur une plateforme dont est doté l'office, est aujourd'hui dépourvue de tout type de signature. Le caractère de fiabilité, d'intégrité et de réalité des données techniques qui sont assises soit sur la signature électronique d'un document, soit sur un certain nombre de données techniques dont la force probante peut être aujourd'hui combattue, se retrouvera dans le cadre d'émissions de constats qui peuvent être sollicités auprès des huissiers de justice. Là, il faut admettre que la matière devient de plus en plus abondante et diverse.

J'ai été dernièrement requis pour déterminer l'intégrité d'un ensemble de messages électroniques, pour savoir s'ils avaient fait l'objet d'une signature ou non, quel était le degré de signature de l'expéditeur, quelles avaient été les conditions de réception de ces messages électroniques par le destinataire. Pouvait-on tracer à la fois l'écriture et les modalités de l'envoi de ce message ? Disposons-nous des outils qui nous permettent, à partir de la trace d'un envoi électronique, de savoir d'où celui-ci est parti et de quel lieu géographique il a été adressé ? C'est la notion de datation atomique ou de localisation GPS d'un mail qui est aujourd'hui techniquement possible. Nous sommes amenés en tant qu'huissiers à constater qu'il est possible de déterminer, à partir de certains outils, qui a été l'expéditeur de ce mail, d'où il est parti géographique parlant et, éventuellement, de quel type d'ordinateur il est parti. Sur le degré de validité et de graduation de la validité des signatures électroniques, je m'en réfère, monsieur le président, à ce que Christiane FERAL-SCHUHL nous a dit.

M. le Président.- Maintenant, le point de vue de l'expert, monsieur Lipski ?

Stéphane LIPSKI.- Merci, monsieur le président. L'expert est pragmatique. Il prend les informations qu'on lui donne. Sa mission sera surtout d'indiquer au tribunal le degré de fiabilité de l'information qu'on va lui donner. Y a-t-il une fiabilité très faible, moyenne ou forte ? On est aujourd'hui capable de faire des investigations assez poussées sur les origines des mails. Sur la datation c'est un peu plus compliqué, mais j'ai vu des cas où l'on a retrouvé l'émetteur d'un mail parce que quelqu'un avait envoyé des mails en pensant que l'on n'était pas capable de retrouver qu'il les envoyait de sa boîte personnelle et de son domicile. Il existe donc aujourd'hui des possibilités d'investigation.

Les informations qui sont transmises, aujourd'hui en tout cas en expertise, ne respectent généralement pas la présomption légale de fiabilité. L'exemple que je donnais tout à l'heure du traitement qui a été retenu pour la signature des rapports du commissaire aux comptes et le système de signature électronique est un traitement tout à fait exceptionnel. Généralement, l'essentiel des communications ne bénéficie pas de ce niveau de sécurité. Il appartient à l'expert, au cas par cas, d'apprécier et d'indiquer quel est le degré de fiabilité de l'information qui sera plus ou moins importante. Ce peut être extrêmement variable. En l'occurrence, on considère aujourd'hui généralement dans les expertises que les informations données, sauf preuve contraire ou mise en cause, le sont de bonne foi et qu'il n'y a pas lieu de les remettre en cause. Mais s'il y a lieu de les remettre en cause et s'il faut aller rechercher les possibilités de modification, malheureusement, les possibilités de modification d'information en informatique sont extrêmement étendues. Plus la personne qui modifie l'information est techniquement compétente, plus ce sera difficile à déterminer, voire pratiquement impossible dans certains cas.

M. le Président.- Maintenant, passons au point de vue du juge.

Emmanuel BINOCHE.- Je voudrais simplement insister sur le fait que l'on parle dans un cas d'une présomption légale de fiabilité, ce qui ne veut pas dire que l'on ne puisse pas aboutir à une fiabilité en dehors de cette présomption légale. Cela paraît une évidence, mais je voudrais insister sur les critères que l'on retrouvera encore plus tard. Nécessaire identification veut dire lien de la personne qui est supposée être à l'origine de l'acte avec l'acte auquel cette signature s'attache, intégrité de l'acte et évidemment conservation si cet élément de preuve est contesté et que l'on souhaite le rechercher. Il peut très bien y avoir une présomption qui résultera d'un certain nombre d'éléments.

Je crois que la jurisprudence entrera nécessairement dans une problématique qui a déjà été plus ou moins rencontrée en ce qui concerne la fiabilité de la signature hors présomption légale avec ce qui a été dégagé en matière de télécopie, de photocopie. Il y aura certaines convergences dont résultera la possibilité d'imputer à telle ou telle personne. On retrouvera également toutes les précautions qui ont déjà été examinées dans les jurisprudences eu égard aux éventuels risques de montage, et ce sera encore la tâche du juge que de vérifier qu'aucun risque de montage n'est véritablement évident à travers les pièces qu'on lui propose.

M. le Président.- La dernière question que je souhaitais poser à propos des difficultés présentes est relative à la conservation de la preuve numérique. Je pose cette question à Me Lotte et à M. Lipski.

Maurice LOTTE.- Aujourd'hui, dans ses rapports avec ses donneurs d'ordre et plus précisément avec les correspondants avocats qui confient à un huissier de justice l'exécution d'une décision, un des principaux sujets qui fera débat est la condition de

transmission du titre exécutoire ou de la décision de justice proprement dite. N'oublions pas que, à l'égard de l'huissier de justice, c'est la détention même du titre exécutoire qui emporte son mandat d'exécution. Sous quelle forme ce titre exécutoire doit-il être transmis ou remis à l'huissier de justice ? Il ne faut jamais perdre de vue qu'à l'égard des personnes envers lesquelles cette décision est exécutée ainsi qu'à l'égard des tiers entre les mains desquels une mesure d'exécution peut également être diligentée, l'huissier doit toujours être à-même, sur-le-champ, de justifier qu'il est porteur d'un titre exécutoire ou d'une décision de justice exécutoire qui lui permet notamment de réaliser les mesures de saisie qu'il est en train d'accomplir. Ce titre exécutoire sera-t-il et peut-il être valablement transmis sous forme numérique à un huissier de justice, à charge pour lui d'en assurer un exemplaire papier sur la base duquel il engagera les mesures d'exécution ?

Pour être franc, la réponse est aujourd'hui négative. Certains avocats transmettaient leur titre exécutoire par télécopie, elle-même issue d'une télécopie avec une signature illisible, une absence de formule exécutoire, une signature du magistrat ou du greffe à peine déchiffrable. Le support numérique, qui a généralement pour origine le même document sous version PDF scannerisé, n'a malheureusement pas de meilleure qualité. Autorise-t-elle un huissier à engager des mesures d'exécution coercitives sur la base de ce seul et unique document ? Aujourd'hui, non. Par définition, un huissier de justice, dans les conditions de conservation des titres exécutoires et des minutes qu'il aura en charge de conserver, doit être porteur d'un original papier.

S'agissant de la question proprement dite des conditions de la preuve numérique, l'huissier de justice sera destinataire, dans le cadre de procès-verbaux de constats, de certains documents simplement parce que des tiers ou parties à titre privé interviendront auprès d'un huissier pour qu'il atteste ou qu'il reçoive en dépôt tel ou tel type de document. Aujourd'hui, en cette matière, les supports et les natures de documents sont divers et variés. L'huissier dispose-t-il aujourd'hui des outils techniques qui lui permettent d'assurer la conservation de ces données et de ces documents ? La réponse est "oui" techniquement parce que les outils existent, ils sont tous sur le marché. Ces outils nécessitent-ils et engendrent-ils en eux-mêmes une valeur d'intégrité suffisamment probante pour que l'huissier, parce qu'il les a signés, parce qu'il a attesté du dépôt de ces documents sous telle ou telle forme, puisse les conserver et les faire valoir comme une preuve probante ? Aujourd'hui, la réponse ne peut être donnée que sur la fiabilité des éléments techniques et des outils techniques ouverts à la profession des huissiers de justice. Ces outils, dans leur degré de technologie, sont-ils suffisants ? Je pense que c'est M. LIPSKI qui va nous répondre.

M. le Président.- Justement, monsieur Lipski, vous avez la parole.

Stéphane LIPSKI.- En termes de conservation, deux problématiques sont essentielles, d'une part la date, et d'autre part la capacité de conserver (sous quel délai on peut conserver l'information).

Il n'existe pas de certitude concernant les dates. Si je prends l'exemple de la Compagnie nationale des commissaires aux comptes, pour fiabiliser la date dont on pourrait supposer qu'elle a été manipulée, modifiée par le commissaire aux comptes et transmise avec une date qui n'était pas la réelle date de transmission, un archivage de nos rapports est prévu auprès d'un tiers archiveur. Il n'existe pas énormément de tiers archiveurs. Lorsque l'on utilise la signature électronique, on transmet immédiatement le rapport électronique au tiers archiveur et ceci est horodaté chez le tiers archiveur. On a donc une sécurité par cette conservation auprès d'un tiers. Sinon, on peut très bien conserver l'information, mais on n'aura

jamais la sécurité de la date exacte de l'information, la date de fourniture et de production de cette formation. De même pour l'écrit, je peux très bien aujourd'hui signer en disant : "Paris, le 14 juillet 2007".

La deuxième difficulté en termes de conservation est la durée de la conservation et la qualité du support. Lorsque l'on a un support papier, on est généralement tranquille pour quelques années, pour quelques siècles même si les conservations ne sont pas trop mauvaises. S'agissant des supports magnétiques, la durée de conservation est beaucoup plus courte et dépend très lourdement de la qualité de la conservation. Pour un système de conservation sur support magnétique, la durée de la conservation est de quelques années. Si vous essayez aujourd'hui de relire, à condition d'avoir les outils car cela évolue très vite, une disquette ancienne de quinze ou vingt ans, vous avez toutes les chances d'avoir beaucoup de difficultés pour être en mesure de le faire, car maintes informations seront perdues.

Je rebondis sur ce que disait Me FERAL-SCHUHL : se pose le problème de la reconstitution d'information. Je suis par exemple obligé de relire un fichier texte. Si je n'arrive pas à relire certains bits ce n'est pas très grave, il manquera quelques lettres ou un mot, une phrase. Dans une clé, chaque bit a une signification. Les systèmes de codification sont plus ou moins complexes utilisés avec 128 bits ou 1024. A 1024, avec les outils actuels, il faut des siècles pour arriver à décrypter. Dans dix ou vingt ans, je ne sais pas. Si l'on a un problème sur l'information et que, en tant qu'expert, on me transmet dans six ou huit ans cette même clé et que je n'arrive pas à relire un bit, je ne pourrai rien contrôler. Les sauvegardes sur CD-Rom donnent lieu à inscription, que l'on peut considérer pratiquement comme de l'inscription matérielle, durent des dizaines d'années, mais sans doute pas beaucoup plus qu'un siècle ; on ne le sait pas encore aujourd'hui. Si j'interviens une demi-douzaine d'années après sur un autre support qui a été conservé dans une pièce mal climatisée, je risque d'avoir beaucoup de difficultés pour cette relecture. Un gros problème de conservation de cette preuve numérique se pose effectivement aujourd'hui et je pense que l'on ne prendra conscience des problèmes que dans les dix ou vingt ans qui viennent.

La Compagnie des commissaires aux comptes, en s'adressant à un tiers archiveur qui conserve les informations sur des supports conservés sur une longue durée pour ne pas rencontrer les problèmes que j'ai exposés, a pris une sécurité. La solution informatique est de faire la chose suivante : sauvegarder sur un support et, périodiquement, tous les cinq ans par exemple, non seulement tester, mais recopier sur un autre support de manière à rafraîchir l'information. Ces systèmes sont relativement lourds mais je pense que, petit à petit, il faudra demander aux sociétés de procéder de cette façon. Une des grandes difficultés que nous avons, en tant qu'experts judiciaires, est que nous intervenons naturellement sur des systèmes qui datent de quelques années. La plupart des experts sont incapables de relire un système qui a dix ans. Qui est aujourd'hui capable de relire une disquette 5'1/4 s'il n'a pas conservé le matériel alors que c'était le support habituel il y a une dizaine d'années ? C'est une vraie problématique.

3. Les perspectives

M. le Président.- Nous avons une hiérarchisation dans les écrits sur papier, « de la carte postale à l'acte notarié ». Va-t-on vers une hiérarchisation des documents numériques ?

Christiane FERAL-SCHUHL.- Cela existe déjà dans les documents électroniques puisqu'il est possible d'envoyer un recommandé électronique, il est possible de confidentialiser un document électronique. Il est donc déjà possible de décider d'attribuer un niveau d'authenticité à un document, de qualifier un document électronique pour créer cette hiérarchisation. On a beaucoup parlé de la suppression du papier, mais les entreprises, et chacun de nous d'ailleurs a une propension très claire à multiplier la création d'octets. Imaginez tout simplement que l'on travaille sur un contrat. Avez-vous une idée du nombre de versions que l'on conserve ? En version papier, on conserverait peut-être la première et la dernière version. On ferait ce ménage qui, souvent, n'est pas fait.

Lorsque l'on aborde cette question, on aborde la question plus large du patrimoine informationnel qui n'est pas déconnecté de la politique d'archivage. Sans revenir sur les questions de conservation, une vraie préoccupation, qui doit être celle de chaque chef d'entreprise aujourd'hui, est de savoir ce qu'il faut conserver et ce qu'il ne faut pas conserver. Dans ce qu'il faut conserver, il y a une hiérarchisation entre ce que l'on a envie de conserver à titre informatif, et ce que l'on doit conserver à raison des prescriptions légales, à raison des risques de contrôles dont on peut faire l'objet fiscalement (contrôle de Sécurité sociale ou autres). Toutes ces prescriptions doivent être intégrées dans cette politique d'archivage et vont créer une hiérarchisation par la force des choses puisqu'un délai sera rattaché à la durée de conservation, avec toujours comme préoccupation la possibilité de restituer ces éléments avec toutes les garanties d'intégrité et d'authentification dont on a parlé. Ce qui conduit à s'interroger sur la pertinence des moyens mis en place dans le cadre de l'archivage pour être sûr que cette présomption légale jouera au bénéfice de celui qui souhaitera produire cet élément de preuve.

Je voudrais ajouter qu'il y a une autre préoccupation. Lorsqu'on parle de documents électroniques, il en existe deux types :

- l'écrit électronique, celui qui est créé, celui que je vais signer électroniquement et adresser à M. le Président BINOCHE dans le cadre d'une procédure,

- la lettre que je lui aurai envoyée, que j'ai scannée et enregistrée.

L'écrit électronique et la copie ne sont pas sur le même régime juridique. Là, il y a une hiérarchisation dont il faut également tenir compte parce que, lorsque je scanne un courrier, je suis dans la copie, donc dans le champ de l'article 1348 du Code civil. Je suis dans les limites posées par cet article qui prévoit que, à défaut d'original, la copie, pour pouvoir être retenue, doit être la reproduction non seulement fidèle, mais aussi durable du document original. Ce qui pose ici une question. Il y a des techniques, il y a des algorithmes, la numérisation est possible avec certaines précautions, mais on est sorti de la signature électronique. Sur ce terrain, une hiérarchisation et une préoccupation sont à assurer puisque, pour le chef d'entreprise, il y a au final deux préoccupations :

- La première est d'être en mesure de restituer les éléments dont il aura besoin pour établir la preuve d'un fait ou d'un acte juridique en respectant les conditions légales qui s'imposent ;

- La deuxième sera d'être certain que ces documents seront effectivement conservés pendant toute la durée nécessaire imposée par les textes, mais qu'aucune contestation ne sera possible sur ces éléments, indépendamment du régime dans lequel on sera, celui de l'écrit électronique "original" et la copie de l'écrit proprement dit qui, aujourd'hui, est encadrée par un texte différent.

M. le Président.- Maître Lotte, vous avez un complément ?

Maurice LOTTE.- Il y a bien évidemment une hiérarchisation dans la gestion de ces documents puisque, comme Christiane FERAL-SCHUHL vient de l'évoquer, le fait de passer par la scannerisation de l'original fait que celui-ci passe de la valeur d'original à celle de simple copie. A partir de là, le mode de transmission et le fait que la copie ait été adressée en pièce jointe à un message électronique *via* une signature, *via* un cryptage, *via* une clé privée d'envoi et une clé publique de déchiffrement fera que cette copie deviendra à son tour un original à partir duquel on fera à nouveau une autre copie.

Les outils de conservation spécifiques aux actes d'huissiers sont actuellement archivés sous une forme numérique, généralement du PDF en zip et on passe ensuite par une société de confiance pour l'archivage générique de ces documents. La hiérarchisation viendra simplement de la qualité propre du document, de sa nature même et non pas de la modalité de numérisation et du support sur lequel il est enregistré.

M. le Président.- Monsieur Le Président Binoche, comment le décret du 28 décembre 2005 relatif à la procédure civile a-t-il intégré l'écrit électronique et donc la preuve immatérielle ?

Emmanuel BINOCHE.- Nous nous trouvions effectivement à une certaine époque dans l'attente de textes qui viennent à côté de l'acte électronique tel qu'il a été défini par les différents textes qui ont été cités tout à l'heure. Nous étions dans l'attente de textes de même nature pour l'acte de procédure électronique. Nous avons vu ce décret pris le 28 décembre 2005, qui a eu pour effet d'insérer dans le nouveau Code de procédure civile certaines dispositions prévoyant d'abord le fait que ce que l'on appelle le répertoire général, que les avocats connaissent sous son abréviation RG. Le dossier et le registre peuvent être tenus sur support électronique. Le texte le prévoit expressément. Il est indiqué à ce sujet que le système doit garantir l'intégrité et la confidentialité des éléments qu'ils contiennent et permettre d'en assurer la conservation. Là encore, on retrouve toujours ces mêmes items, ces mêmes critères pour inspirer la confiance nécessaire dans ces documents, dans ces répertoires, dans ces registres.

Autres dispositions plus intéressantes encore : celles prévues avec une date d'application indiquée au 1er janvier 2009. Je ne sais pas si l'échéance sera tenue. On sent actuellement une certaine volonté politique. Après, il y a peut-être quelques difficultés, quelques impondérables d'ordre organisationnel ou qui tiennent aussi à la nécessité de procéder à certains investissements. Par ce décret qui remonte à fin 2005, il était prévu que les envois, remises, notifications, les actes de procédures ou convocations, les rapports (rapports d'expertise en particulier), les copies et les expéditions revêtues de la formule exécutoire pourraient être effectués par voie électronique dans certaines conditions. On prévoyait par ailleurs un élément qui me paraît essentiel : le destinataire doit expressément consentir à l'utilisation de la voie électronique. C'est essentiel parce que nous ne sommes pas encore dans une dématérialisation totale. Cette notion de consentement de destinataire nous fait penser à ce qui est prévu dans le cadre de la transaction en ligne, l'article 1369-2 : le consentement préalable de celui qui est amené à être sollicité en ligne.

Là encore, on est au milieu du gué quant à la dématérialisation parce que l'on instaure tout de même le droit du juge à exiger la production de l'original sur support papier lorsqu'il a été établi de cette manière.

Voilà quelques observations que l'on peut donner à ce sujet. Mais surtout les procédés techniques utilisés doivent garantir la fiabilité de l'identification des parties à la communication électronique, l'intégrité des documents adressés, la sécurité et la confidentialité des échanges, la conservation des transmissions, également la possibilité d'établir de manière certaine la date d'envoi et celle de la réception par le destinataire. On voit bien qu'il n'y a pas de solution de continuité dans l'esprit de ces textes et on voit bien la logique similaire qui sous-tend tous ces textes.

Il faut ajouter pour être complet que, par dérogation, il est toujours possible de faire rentrer en application cet article 73 qui contient beaucoup de dispositions que je viens de rappeler, notamment, au sujet des envois et l'échange de messages, la possibilité de le faire entrer en vigueur auparavant moyennant arrêté du Garde des Sceaux et que l'ensemble soit prévu par une convention agréée de manière ou d'une autre. Les juridictions qui, d'ores et déjà, fonctionnent dans le cadre d'une convention, ont éventuellement vocation à voir la mise en application de ces dispositions avant l'échéance du 1er janvier 2009. Ce serait déjà très bien si l'on pouvait avoir les équipements nécessaires pour y procéder.

Des dispositions viennent d'être prises en matière de procédure pénale par un décret du 15 novembre 2007 et paru au JO du 17, qui fait suite à l'insertion dans le Code de procédure pénal d'un article 803-1. Cet article prévoit lui aussi de procéder à certaines notifications à avocat, par lettre recommandée ou par lettre recommandée avec demande d'avis de réception, mais aussi sous la forme de télécopie avec réception ou envoi adressé par un moyen de télécommunication à l'adresse électronique de l'avocat. Le décret du 15 novembre 2007 (Journal officiel du 17 novembre, n°267) donne des possibilités de communication électronique en matière de procédure pénale, en particulier en matière d'instruction et pour les besoins des expertises pénales entre autres. Il y a donc là aussi des avancées au niveau des textes. Il restera maintenant aux infrastructures à se mettre en place.

M. le Président.- Merci beaucoup. La parole est maintenant à la salle.

Echanges avec l'auditoire

Michel ENTAT, expert en informatique.- Je me projette dans le futur. J'ai bien compris qu'aujourd'hui l'usage du document électronique signé est rare, mais que, néanmoins, cet usage est vraiment sécurisé puisque, en utilisant un certificat de classe 3, on est à peu près sûr de l'authentification du signataire et de l'intégrité du document. Toutefois, pour moi, on a tendance à assimiler la signature électronique à la signature manuscrite et à considérer que le signataire était d'accord avec ce que dit le document. Sans être spécialiste, je crois que les textes aujourd'hui renforcent cette appréciation. Ma préoccupation est que la signature électronique se fait non seulement avec un certificat, mais au travers d'un dispositif de signature qui rend le processus très différent de la signature manuscrite. On avait un parapheur, on tourne les pages, on paraphe en bas de chaque page et l'on sait ce que l'on signe. Avec la signature électronique on a un fichier, on choisit même son fichier et à ce moment, selon le logiciel, le fichier apparaît ou n'apparaît pas à l'écran, mais de toute façon pas dans sa totalité. C'est à l'écran et on signe en indiquant son code PIN comme pour la carte bleue. Je me demande si on ne sera pas amené à évaluer la réelle volonté du signataire par rapport au contenu du document.

M. le Président.- Merci monsieur. Le magistrat va vous répondre.

Emmanuel BINOCHE.- L'article 1108-1 dit très clairement : *"Lorsqu'il est exigé une mention écrite de la main même de celui qui s'oblige* (c'est-à-dire qui contracte une obligation)*, ce dernier peut l'apposer sous forme électronique* (ce n'est évidemment pas sous forme manuscrite) *si les conditions de cette apposition sont de nature à garantir qu'elle ne peut être effectuée que par lui-même."* Cela veut dire que là, encore, on fait le lien entre l'auteur de la mention et la mention elle-même. On en déduit qu'elle consent à ces termes, mais c'est le critère qui est déterminé et qui n'est pas différent de celui qui existe lorsqu'il s'agit d'une mention manuscrite, puisque l'idée de la mention manuscrite est d'avoir la présomption la plus grande par le fait qu'il a pris son stylo et que, dans le prolongement de sa main, le stylo a rédigé une phrase que n'a pas rédigée une dactylographe ou quelqu'un sur son traitement de texte. C'est le même esprit qui préside à ce type d'écrit électronique portant mention supposée émaner de la main de son auteur.

Jacques HUILLIER, avocat, membre du Conseil de l'ordre.- J'ai été chargé par le Bâtonnier de m'occuper de la communication électronique. A quoi servira concrètement la signature électronique ? Maître Lotte rappelait que, pour la signification d'un acte, on ne pourrait jamais signifier un acte par voie électronique, sauf à supposer que tout le monde est équipé d'un système informatique, il y aura toujours au bout du bout de la chaîne un support papier pour délivrer l'acte, pour signifier l'acte sur un support papier, quel que soit l'état d'avancement de l'électronique. A terme, est-ce que la signature électronique pourra avoir une utilité concrète , étant entendu que nous échangeons aujourd'hui tous des milliers, des milliards de communications électroniques confidentielles, secrètes, par un système non sécurisé, par l'Internet sans, jusqu'à présent, qu'aucun problème n'ait été rencontré ?

Me Maurice LOTTE.- Je rappelle rapidement qu'il est bien évident que, lors de la rédaction et de la signification d'un acte, l'huissier de justice qui remettra la copie de cet acte ne peut remettre qu'un support papier puisque la validité de cet acte ne résultera que des

conditions de signification. Il y a donc un rapport en face à face avec le destinataire de l'acte. Je le lui remets, éventuellement il m'en donne récépissé ou visa et je reproduis. C'est là que la signature électronique prendra son sens, ses modalités de signification dans mes originaux. Mes originaux, eux, seront conservés sous forme numérique. Ils sont signés numériquement, conservés dans les conditions que j'évoquais tout à l'heure par un tiers archiveur de confiance dans ce que l'on appellera à terme à la Chambre nationale des huissiers de justice le minutier central. La signature ne vaudra que dans la certification du signataire de cet acte qui certifie l'intégrité de son contenu dans le cadre des communications, notifications et transmissions du second original de l'acte d'huissier une fois les formalités de signification accomplies.

Bien évidemment, dans le cadre de l'accomplissement de la signification de l'acte, qui est l'étape qui donnera toute sa valeur et tout son sens à l'existence de l'acte d'huissier, la signature électronique n'a pas de sens. Elle n'a de sens qu'ultérieurement, après régularisation de l'acte dans les conditions de transmission et de communication aux parties et aux tiers.

Bernard DELAFAYE.- Je voudrais rebondir sur ce que vous venez de dire, maître Lotte. Vous avez dit très justement qu'il fallait un contact physique, vraiment réel pour que vous accomplissiez votre finalité, et qu'une seule chose pouvait le permettre : le support papier. Je vous signale que le "P" de PRESAJE est "Prospective". Je ne vais donc pas me contenter de la photographie du passé et peut-être du présent que vous venez de nous fournir. Je voudrais me projeter dans l'avenir et je me pose la question de savoir si nous ne sommes pas, vous comme tous ici pratiquement, un peu trop conservateurs ? Est-ce que, un de ces jours, ne va pas sonner le glas des règles actuelles de signification des actes ? Est-ce que, un de ces jours, ne va pas sonner le glas du support papier comme essentiel à la mission des huissiers de justice ?

Me Maurice LOTTE.- Vous avez raison. Le "P" de PRESAJE est "Prospective" et les huissiers, malgré l'aura de vieille profession, de partisans du papier, des vieilles formules et du vocabulaire obsolète, sont sur ce sujet aujourd'hui dans une véritable volonté de modernité. Je partage complètement votre sentiment s'agissant des règles de signification des actes associées au support qu'est l'acte d'huissier. Ne perdons toutefois jamais de vue que "les actes d'huissiers" ont une immense diversité.

Je veux bien que l'on parle beaucoup de prospective. Malgré tout mon degré de réflexion, comment faire en sorte qu'une mesure de saisie-vente, qu'une mesure de saisie-appréhension d'un véhicule terrestre à moteur et, au-delà, une mesure d'expulsion, puissent se faire sans règle de signification autre qu'un déplacement, d'un contact physique de l'huissier avec le destinataire ou la partie ou la personne qu'il est en charge d'exécuter ou à l'égard duquel il faudra mettre à exécution la décision de justice ?

S'agissant des actes à caractère informatif, les assignations, les significations de décision, ce serait envisageable. S'il nous est demain possible d'adresser par voie électronique la signification d'un acte à un destinataire sous la réserve que celui-ci ait fait valoir son consentement pour le recevoir sous cette forme et que nous ayons en échange à cet envoi un accusé de réception, un récépissé daté, heuré qui nous permette d'attester sans aucune contestation que l'acte a été régulièrement sinon signifié, au moins transmis dans des conditions non contestables, bien sûr, pourquoi pas ? Même en matière de voie d'exécution il y a vis-à-vis des mesures d'exécution à l'égard des tiers les procédures de saisie-attribution. Pourquoi ne pourrions-nous pas également envisager, au même titre que le font le Trésor public dans le cadre des avis à tiers détenteur ou les offices de protection sociale dans le cadre des oppositions à tiers détenteur, la possibilité de transmettre ces actes d'exécution - qui ne

sont aujourd'hui encore que de la seule et unique compétence de l'huissier de justice, au tiers sous cette forme ?

François BOUCHON.- Je continue sur la prospective. Excusez-moi, je ne vois pas tellement l'avenir du papier. Je prends un cas que nous connaissons tous : procès-verbal de stationnement, on ne paie pas tout de suite. On transmet à un huissier pour le recouvrement. L'Administration dispose des relevés et références bancaires. Tout peut donc fort bien se passer complètement par électronique…

Me Maurice LOTTE.- Je vous arrête. Vous êtes dans une matière où l'intervention de l'huissier de justice est inexistante. Le débat sur ce thème spécifique de recouvrement des amendes est intéressant puisque c'est peut-être un des domaines dans lequel l'huissier de justice intervient, oui, mais de manière exclusivement dématérialisée. Il est quasiment virtuel. Nous avons déjà le titre exécutoire émis par le service des amendes du Trésor public dont on sait qu'il n'est lui-même que virtuel, titre collectif, dématérialisé. Ensuite, les services du Trésor public, *via* éventuellement certaines plateformes d'agences de recouvrement, derrière lesquelles on a, ou pas, des huissiers de justice, vous transmettront par voie dématérialisée, par mail ou par courrier qui vous dira : *"Je suis chargé de procéder au recouvrement"*. Vous payez et c'est fini. Il n'y pas de signification, il n'y a pas d'acte d'huissier, pas de responsabilité ni civile ni financière. On est parfaitement en dehors de l'exécution d'un titre exécutoire en matière civile et commerciale.

Jacqueline DERAY, informaticienne.- Je suis expert en informatique auprès de la cour d'appel de Versailles. Je rejoins la prudence de M. LIPSKI en matière de support magnétique et d'informatique. Nous avons aujourd'hui deux populations : les entreprises, les administrations qui sont extrêmement averties et le grand public qui, lui, est extrêmement fragile.

Je citerai un seul cas où l'on se trouve dans ce que définissait Me FERAL-SCHUHL : le milieu du gué. J'ai découvert un site de l'Education nationale dans lequel des inscriptions formelles à des concours étaient uniquement matérialisées par l'impression d'un document. Or, il n'y avait aucun trace de fin de transaction, aucune assurance que les documents étaient vraiment émis et, pour de braves jeunes gens, pourtant férus d'informatique et justement férus d'informatique, le mariage entre le papier et l'électronique n'apparaissait pas évident. Il n'y a pas eu, je pense, auprès des tribunaux administratifs de plainte, mais c'est un exemple d'aberration complète dans le grand public de laisser à des gens moyennement informés des mérites du traitement de l'information.

Michel ROUGER, président de l'institut PRESAJE.- Avant que la table ronde ne se sépare, je voudrais donner quelques informations sur l'origine de la deuxième table ronde. Cette deuxième table ronde nous est venue par l'intermédiaire de ce jeune magistrat Thomas CASSUTO, vice-président au TGI de Nanterre, qui nous a fait connaître Alexis RIMBAUD, l'auteur de l'ouvrage sur lequel nous allons venir autour de cette table ronde. J'ai personnellement été étonné lorsque j'ai vu dans quelles conditions le développement de toutes les techniques de numérisation et toutes les techniques de stockage des informations avait entraîné des modifications plus que substantielles dans les investigations faites au cours des procédures pénales, qu'il s'agisse de délits de type financier ou de crimes de sang. Comme Alexis RIMBAUD, l'auteur du livre, est beaucoup intervenu pour de nombreux juges d'instruction ou pour de nombreux services de police dans la réalisation de ces investigations, nous avons pu constater, lorsqu'il nous a présenté les premiers éléments de son futur ouvrage, qu'il y avait un vrai débat à ouvrir, d'autant plus que, vous le savez tous, les expertises qui

peuvent découler des enquêtes faites dans les procédures pénales n'ont pas de caractère contradictoire, à tout le moins au moment où elles sont réalisées. Il y avait donc véritablement à poser sur la table les conditions dans lesquelles ces opérations se faisaient pour la sécurité des justiciables que nous sommes tous.

C'est là l'origine de cette deuxième table ronde qui va se dérouler sous l'autorité de Thomas CASSUTO.

(Fin de la 1ère table ronde)

2ème table ronde : Expertise numérique et procédure pénale, sous la présidence de M. Thomas CASSUTO

M. le Président.- Mesdames et Messieurs, vous avez bien compris que le numérique est un vecteur formidable d'information et qu'il est l'instrument ou l'accessoire du criminel. Il est aussi l'indice de ses méfaits, et c'est ici que commence le travail nécessaire, de plus en plus nécessaire de l'expert pour participer à la manifestation de la vérité. Nous avons aujourd'hui une table ronde exceptionnelle par sa dimension et par sa qualité. Ses participants vont nous présenter les différents aspects de la preuve numérique en matière pénale. Nous avons essayé d'élaborer une sorte de plan qui respecte la logique du processus judiciaire.

Alexis RIMBAUD, vous êtes spécialiste des nouvelles technologies et vous disposez déjà d'une grande expérience dans ce domaine. Vous avez été désigné en qualité d'expert par de nombreuses autorités judiciaires. Vous nous avez livré dans l'ouvrage de l'institut PRESAJE *Le juge pénal et l'expert numérique*, publié chez Dalloz, un éclairage original sur les nouveaux enjeux de l'expertise, notamment au travers de l'expertise numérique. Pouvez-vous nous présenter, nous rappeler ces grands enjeux ?

Alexis RIMBAUD.- Merci, monsieur Cassuto. J'ai effectivement la lourde responsabilité d'assurer régulièrement l'expertise pénale dans le cadre de ma mission depuis presque dix ans. J'ai accumulé au travers de cet exercice une petite expérience de la preuve numérique. J'ai souvent été confronté au concret, au terrain, aussi à de grandes problématiques qui se posaient, et je dois dire que la rédaction de cet ouvrage m'a fait prendre conscience de certaines difficultés du positionnement de l'expert qui est, pas toujours mais souvent à l'origine de la preuve numérique. Nous avons la lourde tâche d'en gérer et d'en produire. Dans les deux cas, une méthodologie est à appliquer.

Il est vrai que, s'agissant de mon travail régulier, je m'occupe d'affaires pénales souvent très lourdes, je suis régulièrement appelé à la barre. Dans ce cas, la parole de l'expert a un certain poids, même un poids certain. J'ai établi au cours des années une méthodologie qui vise non seulement le contexte de la preuve numérique mais aussi le traitement, les modalités de cette preuve, et je vais essayer de vous faire part de quelques éléments sur l'origine du fait numérique.

On est là presque face à une dichotomie. Il faut attribuer, garder le travail de l'expert au sein d'un contexte de savoir et essayer de le séparer le plus possible du contexte du pouvoir. C'est dans ce dialogue entre le pouvoir et le savoir que le fait numérique peut prendre sa forme. C'est même dans ce dialogue que l'on peut obtenir un résultat intéressant et probant. J'insiste sur ce dialogue.

Pour ma part, je pense qu'il faut le plus possible favoriser le dialogue. L'expert fait, bien sûr, partie du monde du savoir, mais il doit constamment dialoguer, apporter son savoir au pouvoir. Il a un rôle de formateur. Il a rôle, quelles que soient les juridictions, que ce soit l'instruction ou le jugement, de pédagogue. C'est dans ce contexte que la preuve numérique prend tout son sens. Pour être plus concret, une trame définit de mieux en mieux la preuve numérique.

Cette trame commence par l'origine du fait. C'est avant tout autour de l'origine du fait que nous pouvons définir, commencer à définir la preuve numérique. L'origine du fait est une étape extrêmement importante du travail, car on définit à ce moment le contexte de la preuve numérique. C'est le moment pivot où l'on pourra obtenir un résultat intéressant, où l'on récupère auprès des magistrats les éléments probants, les éléments que l'on va analyser. Dans un dialogue constructif, on peut même échanger avec les magistrats pour construire la mission de l'expert, encore une fois dans un but pédagogique, on vient apporter un savoir à toutes les juridictions de façon à constituer des éléments de sa mission. On essaye de comprendre l'origine du fait. On essaie aussi d'en définir le contexte et le contexte historique.

Par exemple, avoir à analyser un fait qui s'est produit sur un réseau informatique oblige évidemment à définir un historique : l'histoire de ce réseau, comment il a été fabriqué, quelles défaillances éventuelles ont été reconnues par les différents fabricants de ce réseau. Quand il s'agit de logiciels, il faut évidemment avoir une connaissance extrêmement approfondie des différentes versions des logiciels, quels logiciels ont fait état de dysfonctionnements avérés, les dernières mises à jour ont-elles été appliqués, etc. ? Je citerai quelques affaires qui m'ont été confiées où l'origine du fait était un élément fondamental de mon analyse comme par exemple des affaires sur des GPS défectueux ayant causé des accidents, etc. Il fallait évidemment revenir en arrière, connaître le fabricant, etc.

Ensuite, on attaque la méthodologie et les outils de préservation du fait. A partir de là, on se trouve dans un contexte pénal assez classique de préservation du fait, de préservation de la preuve. Nous parlerons dans ce colloque de la préservation de la preuve numérique. Sur le concret, de nombreux outils ont été évoqués en première partie : les outils de préservation qui permettent de copier les disques durs, de copier des éléments de stockage numérique, etc. Ces outils sont à la disposition de tous, mais un mode opératoire est aussi extrêmement important. Le rôle de l'expert et du contexte de la preuve numérique est également important dans la partie humaine de la gestion de la preuve numérique.

A été évoquée en première partie la présence d'un huissier pour administrer la preuve numérique. L'expert doit à ce moment se prononcer sur la méthodologie utilisée par l'huissier mais aussi sur la méthodologie utilisée par éventuellement l'informaticien, le directeur des systèmes d'information qui a créé cette preuve. Le positionner dans la mission fait également partie du rôle et de la définition de la preuve numérique. Vient ensuite l'établissement de la méthodologie de l'expertise du fait. C'est extrêmement important et je crois, pour reprendre le but premier de PRESAJE, que c'est sur ce point que les choses vont maintenant évoluer. Des méthodologies existent. Une certification ISO 9000 sur la méthodologie de l'expert devient de plus en plus répandue. C'est presque une obligation. Faire état d'une méthodologie est indispensable, mais la certification, au-delà des méthodes d'inscription de différents organismes, la norme ISO 9000 gagne le monde de l'expertise et permet aussi aux différents intervenants (comme les avocats) de connaître la qualité de la méthode utilisée.

Ensuite, l'expertise sous le sceau du serment proprement dite. Il faut tout de même définir ce qu'est un expert à ce moment précis de la procédure. L'expert n'est pas un technicien. Son rôle est extrêmement défini. Nous avons aussi ce rôle d'échange, pédagogique, d'explication. Depuis l'instauration de la LOLF, nous avons aussi la responsabilité de la gestion de notre l'intervention qu'il faut deviser avant de commencer à travailler.

Enfin, l'administration des résultats est extrêmement importante parce qu'il ne suffit pas de faire état des faits pour les expliquer. On demande souvent à l'expert et à l'expertise numérique en général d'avoir un rôle binaire dans le fait. On pense souvent que l'expert va nous affirmer, nous confirmer, nous infirmer des faits. Or, il faut comprendre que l'expert n'est pas toujours là pour faire ce genre de travail. C'est plutôt le travail d'un technicien. L'expert est aussi là pour créer une hiérarchie dans le fait et des pyramides de responsabilité sur l'affaire qui lui est proposée. Les affaires de pédophilie sont par exemple typiques de ce genre de cas. Dans ce cas l'expert a les éléments, il va les faire apparaître, mais il est beaucoup plus important dans son rôle et dans le fait numérique à ce moment de créer une hiérarchie chez l'utilisateur et de savoir définir comment, pourquoi, à partir de quel moment ces images ou ces éléments sont arrivés sur l'ordinateur. Y avait-il une volonté réelle de la part de l'utilisateur ? Il convient de se méfier d'un positionnement binaire de la preuve numérique. Bien sûr, c'est du numérique, mais l'expert est avant tout là pour créer une hiérarchie sur le fait, évidemment avec son savoir technologique, mais il est là à charge et à décharge. Il est loin du pouvoir. Il est tout simplement là pour faire état des faits.

M. le Président.- Merci, Alexis. On comprend bien qu'il y a une dimension analytique et surtout qu'un vrai dialogue, en tout cas du point de vue de l'expert, est nécessaire entre le juge et l'expert pour construire la mission d'expertise et construire, préparer à un résultat qui pourra être exploité, puisque la vocation du juge d'instruction est de pouvoir délivrer un produit fini qui soit jugeable par une juridiction.

Chère Laurence IFRAH, vous êtes criminologue, spécialisée en criminalité numérique au sein de l'université Paris II - Assas et vous connaissez très bien les grandes tendances de ce phénomène. On peut se demander si la première difficulté n'est pas de vivre dans un univers compromis.

Laurence IFRAH.- Merci, monsieur le juge. Je voulais d'abord faire un point sur l'état des menaces, qu'elles soient situées dans les entreprises ou dans des institutions publiques. Au-delà de nos discussions aujourd'hui, un autre problème vient du fait que les dirigeants, les responsables refusent, face à un incident, d'entamer des poursuites, de déposer une plainte pour diverses raisons. C'est ce que je vais essayer de vous expliquer.

On considère trois formes essentielles de menaces :

- celles que je qualifierais de volontaires, c'est-à-dire un acte avec une intervention spécifique : une proposition financière émise par un concurrent ou par divers acteurs, un départ qui se serait passé dans de mauvaises conditions ou, même s'il se passe dans de bonnes conditions, des cadres partent fréquemment avec les dossiers de l'entreprise parce qu'ils vont continuer à travailler dans le même secteur d'activité et cela leur donnera de bonnes bases pour démarrer leur nouvel emploi ;

- l'acte de vengeance où l'acteur qui aura commis l'acte n'aura pas forcément pris la mesure des enjeux et des risques qu'il prend.

J'ai rencontré la semaine dernière l'exemple d'une entreprise d'une centaine de personnes dont le réseau a été entièrement détruit par l'administrateur-système qui a été licencié. Comme il était au cœur de la machine informatique, il s'est allègrement vengé et a détruit l'intégralité du système. Il n'y avait donc plus de données et plus d'archives. Dans cette même entreprise, les responsables avaient pris soin de mettre les mots de passe du serveur dans un coffre ignifugé, mais le serveur lui-même n'avait aucune protection contre le feu ou quoi que ce soit. Sans serveur, le mot de passe ne sert à rien.

- Viennent ensuite les menaces involontaires. Je vous parle de pressions. Les pressions ont surtout été vues dans les groupes bancaires qui ont subi des actes de malveillance où des virements ont été faits. Il a été constaté que, fréquemment, une personne en interne avait été complice d'un acte, c'est-à-dire l'installation d'un cheval de Troie, un programme qui permet de récupérer des informations à distance. Ces pressions sont souvent exercées physiquement sur la famille de la personne contactée et il est difficile de lutter contre parce que les gens ont peur. Ensuite le téléchargement. J'appelle involontaire un téléchargement car, parfois, les utilisateurs des systèmes d'information n'ont pas conscience des sites qu'ils vont consulter, soit en regard de leur activité, soit parce qu'ils vont prendre quelques instants pour se délasser. On pourra télécharger des outils, des fichiers qui seront *a priori* innocents mais qui, en réalité, contiendront divers chevaux de Troie ou virus pas forcément détectables par les systèmes de protection mis en place dans les entreprises.

Un nouveau fait assez récent est très important : ce que l'on appelle les réseaux sociaux. Il s'agit d'un site Internet sur lequel on va décliner son identité, faire son portrait, son parcours scolaire, professionnel. Au départ, cela part d'un très bon sentiment. L'objectif était très sain à la première approche puisque cela vous permet de retrouver des gens que vous n'avez pas vus depuis des années, physiquement ou professionnellement éloignés. C'est très bien, mais on se retrouve aujourd'hui face à un énorme problème. En France, plus de 700 000 personnes sont inscrites sur le plus célèbre site (facebook), dans lequel on peut récupérer toutes les informations concernant une personne, ce qui permet, par des moyens détournés, de focaliser sur une cible et d'aller passer par un contact différent. On verra qu'une personne a un ami proche dans telle région. On va prendre son identité et lui envoyer un e-mail avec un sujet qui la concernera forcément puisque tous les dialogues sont transcrits sur le site. La personne l'ouvrira puisqu'elle connaît l'expéditeur et le fichier sera piégé. Là, on tombe sur un problème de confidentialité des données et de fuite d'information.

Les menaces détournées sont tout ce qui concerne les périphériques, notamment les clés USB des ordinateurs portables dont on peut recopier le contenu ou tout simplement le dérober. Je constate quasiment tous les jours que, quand des gens me donnent une clé USB pour récupérer un fichier, cette même clé contiendra tous les documents essentiels sur lesquels ils travaillent tous les jours, souvent très sensibles. Des programmes facilement et gratuitement téléchargeables sur Internet permettent, pendant que, sur votre ordinateur, vous verrez le contenu de la clé USB, d'installer le fichier désiré. Sur la clé USB, en transparence, un programme se chargera d'aspirer tout le contenu de la clé. Vous ne le voyez pas, mais cela se fait et fonctionne très bien.

Il existe également des salariés malveillants. La récupération d'outils pour contourner les mesures de sécurité, quand les entreprises en ont, se fait, c'est courant ; on le voit régulièrement. On essaye d'établir un contact privilégié avec l'administrateur système. Cela permet aussi d'obtenir quelques faveurs et des connexions qui sont parfois interdites.

Le plus difficile, ce sont les outils que l'on appelle *anti-forensic* qui empêchent les experts de procéder à leur travail : modification des dates de création et de visualisation des fichiers - nous n'avons rien pour lutter contre - ou tout simplement des effacements particulièrement sécurisés.

Je vais vous expliquer pourquoi les dirigeants, les responsables ne portent pas plainte. Le dirigeant, par essence, n'a pas compris et ne veut pas comprendre l'ampleur de ce que cela peut représenter. Il refuse de s'intéresser à l'outil informatique et va déléguer tout cela à un collaborateur qui aura lui-même soit un administrateur-système, soit un ami qui a des

connaissances en informatique et qui tentera d'installer un système plus ou moins sécurisé. Ce système sera effectivement adapté à un budget que l'on aura confié. Mais les questions que l'on devrait se poser sont : Que dois-je essentiellement protéger ? Qu'est-ce qui a de la valeur ? Qu'est-ce qui me met en risque ?

En cas de constat d'incident, on appelle tout le monde au secours. La prévention ne fonctionne pas dans ces cas-là. On évalue l'étendue des dégâts, on appelle les experts et on refuse de porter plainte parce que l'on n'est pas en conformité avec les fichiers vis-à-vis de la CNIL, on a peur de perdre son image vis-à-vis de la concurrence, la crainte des représailles des salariés parce que, quand un salarié s'est fait prendre, les autres ne considèreront pas forcément ce qu'il a fait comme un acte vraiment malveillant pour l'entreprise. S'il a beaucoup d'amis dans l'entreprise, cela créera des tensions. Dernier point, surtout, il n'y a pas de charte d'utilisation des systèmes d'information. Il est donc en faute et il va étouffer. Après l'incident, on va sécuriser puisque l'on a fait appel à des experts, ce qui est très mal vécu parce que pris comme une atteinte à la liberté. Les salariés avaient l'habitude de s'épanouir en regardant Internet, une « sensation de flicage » et on sera observé, espionné. Il y a donc un refus de signer la charte et une rancœur se crée vis-à-vis de la direction.

La solution est de le déculpabiliser et, ainsi, on arrive à établir un dialogue, ce qui est important. Expliquer au chef d'entreprise et à ses équipes que cela arrive dans les réseaux les mieux protégés. Voici un exemple d'un document "confidentiel défense" émanant du cabinet du Premier ministre le 10 août 2005, que j'ai récupéré sur Internet et qui circulait librement dix-huit jours plus tard. Les autorités fiscales britanniques ont annoncé hier la perte de fichiers de données fiscales de 25 millions d'Anglais avec toutes les conséquences possibles de fraudes bancaires et d'usurpation d'identité. La solution est également de faire une séance de sensibilisation : expliquer, engendrer un débat, une discussion, insister aussi sur le fait que l'entreprise est obligée, au regard de la loi, de prendre ses précautions et ses mesures pour ne pas s'attirer les foudres des salariés et les rassurer.

M. le Président.- Merci, Laurence IFRAH.

Chacun comprend bien que nous sommes dans un environnement hostile, dans lequel les acteurs, par manque de prévoyance ou de prévention, s'exposent au risque de malveillance à caractère informatique. C'est lorsque l'événement survient, que l'on se pose la question de la réponse. Maître Alain Bensoussan, vous êtes un spécialiste connu et reconnu des technologies de l'information et de la communication. Vous êtes naturellement un interlocuteur privilégié de ces entreprises, des victimes, qui constatent cet événement indésirable. Comment l'avocat peut-il orienter la bonne mise en état de la procédure au regard justement de cet environnement qui d'ailleurs, au sein même de l'entreprise, est souvent dégradé ?

Alain BENSOUSSAN.- Je vous propose un rêve et un cauchemar pour l'expertise numérique et la procédure pénale. Pourquoi un rêve ? Tous les dispositifs légaux sont opérationnels. Un vrai bonheur ! Au niveau mondial, des conventions internationales dans la plupart des pays. La controverse, c'est qu'*a priori* il y a de la fraude informatique partout depuis 1988, depuis la loi Godfrain.

La fraude est d'autant plus facile maintenant, quasiment tout le monde est capable de frauder, et les outils sur le système Internet disponibles à qui veut. La fraude est ouverte pour tous. On pourrait penser qu'à ce moment un malheureux avocat pourrait travailler dans ce domaine et développer une compétence. En réalité non parce qu'il n'y a pas d'affaires.

"L'informatique, enjeu de la fraude ?" aurait été un premier élément de spécialité. "L'informatique, objet de la fraude ?" un second. On peut frauder pour faire des infractions, les infractions elles-mêmes sont des infractions informatiques.

Le cadre juridique est merveilleux. Vous avez un ensemble d'infractions informatique et libertés. Vous avez même des infractions dans le domaine informatique et libertés qui existent et qui s'appuient sur des textes qui n'existent plus. La loi relative à la fraude informatique parle des fraudes informatiques, mais n'utilise jamais le terme. Peu importe, au fond. On a aussi les interceptions de télécommunications, tout ce qui est autour de la signature et de la défense nationale. La défense nationale a des textes spécifiques pour la fraude informatique. On pourrait concevoir qu'elle pourrait utiliser les textes généraux, non. Il existe aujourd'hui du droit pénal de défense nationale et du droit pénal de l'intérêt national, deux ordres publics distincts avec chacun ses infractions. Enfin, avec la loi pour la confiance avec le numérique, tout le monde aura sa fraude en termes d'octets, des textes avec des infractions associées.

Plus d'une centaine d'infractions moins une : le vol d'information. Cela n'existe pas. Pour le reste, tout existe et on a des textes. Regardez, sur ce site, on trouve "comment fabriquer une bombe ?". J'ai à la fois la fabrication de la bombe et l'infraction pénale qui interdit l'information pour la fabriquer.

Pourquoi n'y a-t-il pas d'affaires puisqu'il y a tant de fraudes ? On a une justice électronique complète avec sa police et sa gendarmerie. On dispose aujourd'hui de textes sur la planque informationnelle, sur la filature informationnelle, sur la perquisition numérique, sur l'interrogatoire à distance, sur la traduction et sur la saisie électronique, issus des lois Perben 1, Perben 2, et des Sarkozy 1 et 2. Nous sommes en avance en matière de droit électronique sur les faits. Pour une fois, les juristes se conjuguent au temps futur.

Alors, d'où vient le problème ? Où sont les freins ? Le premier, ce sont les casiers en ligne. J'ai par exemple le problème de l'indemnisation de l'action judiciaire, une demande en cours où j'ai mis une décision de la CNIL, une décision importante de la CNIL sur mon site web et le justiciable dit : *"vous ne devez pas publier cette décision parce qu'elle n'est pas anonymisée"*. Ces décisions judiciaires qui se trouvaient avant face à une victime indemnisée se retrouvent en fait en une "victime publicité" si vous me permettez ce terme. Le premier grand frein, c'est que, gagnant ou perdant, ils ne veulent pas de bruit.

Le deuxième élément qui bloque, c'est informatique et libertés. Dans informatique et libertés, vous avez trois points.

- Une personne qui se fait détourner son fichier est punissable de fraude par défaut de sécurité parce qu'elle n'a pas pris toutes précautions utiles. On a déjà une décision de quelqu'un qui s'était fait détourner son fichier. Il est allé voir son avocat qui a porté plainte, et c'est lui, l'accusé, qui s'est trouvé en position d'infraction.

- La plupart des détournements de fichiers sont des détournements de fichiers avec des données numériques. Ces données numériques ne sont pas déclarées. Ainsi, par exemple, derrière 90 % des fraudes il y a un salarié. On est très proche d'un abus de confiance. Mais l'abus de confiance n'est rien à côté de la déclaration CNIL. Vous encourez 5 ans si vous ne déclarez pas un fichier, contre 3 ans pour un abus de confiance.

- Enfin, dernier élément, la sécurité déclaration. C'est aussi la problématique que vous avez indiquée de la charte informatique.

On va pouvoir saisir ces mails. Mais, à défaut de charte, ils relèvent tous de la vie privée. Si vous les regardez, vous êtes non seulement en face d'une interception de télécommunication ou une violation de la correspondance privée, une déclaration sans droit ni titre des formalités préalables et, bien entendu, un manquement à la sécurité. Le dernier élément, ce sont les référentiels de bonne pratique. Messieurs les experts, c'est vrai, j'aime à dire dans ce domaine que la science se démontre, mais, à l'audience, l'avocat résiste un peu. Il n'empêche qu'il n'y a pas de référentiel méthodologique. Il n'y a pas, dans ce domaine, la possibilité de traçabilité de ce que fait l'expert. Il n'y a pas de réversibilité, il n'y a pas de preuve absolue de non-contamination de la donnée d'octets. C'est donc, là aussi, un enjeu extrêmement important, d'autant que les parties ont tendance à regarder un peu avant que la police n'arrive et que l'instruction ne débute, faisant que la preuve se trouve contaminée.

Méthodologie, traçabilité et contamination sont souvent un des freins au développement de l'expertise pénale. Les parquets sont extrêmement motivés pour ces affaires, mais il y a peu d'affaires. La question est mondiale. La plupart des textes sont de même nature. Il n'y a donc pas de rupture au niveau international. L'informatisation est la même. Sur la signature électronique, on utilise tous quasiment les mêmes algorithmes. L'universalité est la conséquence du fait que, quand on est techniquement identique, on est souvent juridiquement identique parce que les lois, différentes, ont tendance à recopier sur des contraintes techniques plutôt que sur des contraintes éthiques.

Enfin, la coopération policière est présente, comme on peut le voir avec les éléments d'Interpol. Une convention internationale permet aujourd'hui, en matière de cybercriminalité, d'agir 24/24, 7/7. Des magistrats d'instruction dans l'ensemble de ces pays sont spécialisés et en relation directe. Il y a donc une réponse internationale.

Il y a une réponse électronique, il y a une réponse technique, il y a une réponse juridique, mais il n'y a pas d'affaires parce que la victime a peur de la double peine. La première est d'avoir été déjà frappé par l'électronique, la deuxième est d'être frappé par la publicité électronique.

M. le Président.- Merci, maître Bensoussan. Vous nous avez donc bien dissuadé, dans l'hypothèse d'un événement indésirable, d'aller déposer une plainte, et vous nous avez bien mis en évidence la nécessité pour l'expert d'adopter un processus dans l'élaboration de son travail qui permette d'avoir une appréhension exacte, qui permette de vérifier la qualité du travail et de déterminer la rigueur du résultat obtenu.

Vous dites qu'il n'y a pas de procédure. Néanmoins, avec Fabien LANG, nous avons eu à connaître en commun des procédures de fraudes informatiques dites *fishing* ou *farming* d'ampleur internationale. En tant que n° 2 de l'OCLCTIC (Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication), vous êtes à la tête d'un service extrêmement compétent avec lequel j'ai eu beaucoup de plaisir et d'intérêt à travailler.

Comment aborder la scène de crime, une scène de crime tout à fait particulière et, plus particulièrement sous cet angle spécifique de la victime qui est tentée de regarder sous le couvercle et donc, déjà, de polluer cette scène de crime ?

Fabien LANG.- Merci, monsieur Cassuto. Je représente l'OCLCTIC qui est en quelque sorte le bras armé de la Direction centrale de la police judiciaire dans le domaine de la lutte contre la cybercriminalité qui recouvre des situations assez diverses. Concrètement, nous sommes compétents pour traiter d'actes classiques de piratage, d'intrusion sur des

systèmes de traitement automatisé de données et, plus généralement, des actes d'escroquerie d'ampleur internationale telles que les affaires de *phishing* ou de *pharming*. Nous sommes également compétents sur le volet des fraudes aux cartes bancaires qui se développent de façon relativement importante. Nous avons d'autres missions en termes de centralisation, de diffusion d'information, nous participons à certains groupes de travail et nous constituons aussi un point de contact dans les échanges internationaux Interpol, Europol.

La problématique de la preuve numérique est pour nous à la fois simple et compliquée. Notre rôle est évidemment de recevoir des plaintes, de rechercher une éventuelle qualification pénale aux faits qui nous sont rapportés et ensuite de localiser et d'identifier l'auteur de cette infraction, puis, sur place, dans le cadre de perquisitions, de rechercher les preuves matérielles de participation de l'auteur aux faits incriminés. Comment procédons-nous concrètement sur le terrain ? Evidemment, nous nous déplaçons chez l'auteur. La première chose à faire, évidente, est de garantir l'intégrité des données qui sont recueillies sur le support numérique. Nous employons pour cela des outils qui sont utilisés par toutes les polices du monde. Il s'agit de bloqueurs en écriture qui empêchent toute modification des données présentes sur le support. C'est là un élément essentiel qui conditionnera la validité de la procédure.

Ceci dit, nous avons actuellement quelques difficultés, notamment avec de nouveaux systèmes d'exploitation tels que Vista où nous ne pouvons plus procéder de la sorte et où nous devons préalablement procéder à quelques vérifications, notamment pour rechercher les clés de chiffrement. Cela occasionne des difficultés nouvelles. Ensuite, nous utilisons des logiciels *forensic* qui nous permettent de rechercher sur les ordinateurs des traces numériques, y compris lorsqu'elles auront été effacées.

Autre garantie pour le procès pénal, ces actes sont faits en présence du mis en cause ou de la personne chez qui la perquisition a lieu. Les actes sont décrits très précisément sur procès-verbal et sont horodatés. La dernière garantie est la formation des enquêteurs spécialisés chargés de ces investigations. Ces policiers ont passé un stage avec succès et sont reconnus comme tout à fait compétents pour recueillir ces preuves.

De façon plus générale, quelles sont nos difficultés actuelles ?

- L'intervention des services informatiques préalablement à celle des enquêteurs peut avoir pour effet de modifier ou de supprimer involontairement certaines traces. Cela arrive très fréquemment et il est parfois difficile, après coup, de rechercher, de trouver des données qui pourront être apportées à la justice.

- L'incohérence des systèmes, notamment l'horodatage des ordinateurs qui peut évidemment poser des difficultés lors d'un procès pénal.

Je rejoindrai ce qu'a dit Me BENSOUSSAN. Les actes existent. Les plaintes sont beaucoup plus difficiles à obtenir. Pourquoi ? Je l'ignore. Je pense que l'analyse donnée à la fois par Mme IFRAH et par Me BENSOUSSAN est bonne : les entreprises victimes peuvent craindre de déposer une plainte lorsqu'elles s'aperçoivent qu'elles sont elles-mêmes en infraction aux règles de la CNIL. Mais plus généralement, je crois qu'il y a une peur en terme d'image. Une entreprise peut craindre une atteinte à son image lorsque les faits sont relayés dans la presse ou sur Internet. On sait que, dans le domaine numérique, l'information passe très vite.

Autre difficulté pour les services de police et de gendarmerie : une enquête se base toujours sur des indices, des traces et des éléments matériels nécessaires à la manifestation de la vérité. Or, en matière de cybercriminalité, ces indices, qui sont le plus souvent de nature électronique, n'ont aucune signification sans l'éclairage du prestataire de service à l'origine d'une communication électronique. Pour exemple, une identification d'une adresse Internet Protocol (IP) passera nécessairement par l'envoi d'une réquisition judiciaire au fournisseur d'accès Internet, qui devra communiquer l'identité du client auquel cette adresse IP a été attribuée au moment des faits. Cela implique donc que ces opérateurs soient soumis à un certain nombre de règles, notamment en matière de conservation de données techniques. La France dispose dans ce domaine d'une législation bien adaptée, ce qui n'est pas le cas dans tous les pays. Aussi, il arrive fréquemment que certaines enquêtes ne puissent tout simplement pas aboutir parce les Etats requis sont incapables de communiquer les données techniques indispensables. Cette situation est très difficile à admettre pour les services de police judiciaire.

- La localisation des bases de données dans des pays étrangers.

Un exemple très concret : vous ouvrez une adresse mail sur Yahoo.com ou sur aol.com, les données que vous allez transmettre seront basées notamment aux Etats-Unis. Cela signifie pour nous qu'il faut nécessairement une commission rogatoire internationale pour obtenir l'identification de la personne qui se sera enregistrée. Nous n'obtenons la commission rogatoire internationale que pour des affaires graves, sensibles, dont le préjudice est important. Pour la plupart des affaires que nous traitons, cela n'arrive pas. De fait, encore une fois, les enquêtes sont renvoyées sous le timbre « vaines recherches » alors même qu'elles ne présentaient pas d'obstacles techniques particuliers.

Dans ce domaine, je pense que quelques évolutions sont à envisager sur le plan du droit international.

La cybercriminalité est internationale, mais on a constaté qu'elle résulte également d'une véritable criminalité organisée. Nous l'avons constaté depuis les années 2000 avec l'avènement d'Internet. Nous avons affaire à des gens qui, techniquement, sont extrêmement compétents, disposent de réseaux, travaillent en réseau et utilisent toutes les ressources actuellement offertes dans le domaine des technologies de l'information et de la communication. Ces équipes peuvent œuvrer depuis la Russie en passant par les rebonds aux Etats-Unis, en Ukraine ou en Chine en utilisant des ordinateurs compromis à travers le monde pour, finalement, aboutir dans notre beau pays ou dans un pays voisin en Europe. Là aussi, on ne peut que constater une distorsion importante entre la fulgurance d'une attaque informatique et le temps de l'enquête, beaucoup plus long. De fait, il s'agit de rassembler en urgence les preuves matérielles et de solliciter la coopération policière internationale, ce qui présente parfois des difficultés, surtout lorsque la gravité des faits ne justifie l'ouverture d'une information judiciaire.

Ce sont concrètement les difficultés qui se posent à nous. Ceci dit, nous disposons en France d'une législation tout à fait adaptée à ces enjeux. C'est sur le plan de la coopération internationale que, véritablement, nous devrons progresser. Je vous remercie.

M. le Président.- Merci, commissaire.

Il est vrai qu'il y a aussi une difficulté : trouver des services compétents pour préserver l'intégrité de la preuve. Nous avons l'exemple d'un service hautement compétent,

mais évidemment, bien souvent, le fait d'aller saisir, déposer une plainte dans un service de moindre compétence peut également poser des problèmes sur la préservation, l'intégrité ou la manière dont la preuve sera exploitée. Là aussi, il y a un effort de moyens pour renforcer la diffusion des compétences dans le domaine des investigations. Il est vrai que, sur le plan international, on pourrait développer. Une commission rogatoire internationale aux Etats-Unis est non seulement une démarche complexe, mais, en même temps, c'est une démarche juridique parce que cela dépendra du lieu où la commission rogatoire internationale sera sollicitée, sera mise en exécution. Entre l'Ouest des Etats-Unis et l'Est, il peut y avoir des différences. Nous avons aussi ce type d'obstacle à surmonter. Nous voyons que l'intégrité de la preuve numérique est nécessaire. Encore faut-il, pour le juge, envisager son exploitation, le cadre de son exploitation.

Monsieur le président Didier PELTIER, vous êtes chargé de l'instruction au pôle santé publique à Paris. Vous connaissez un contentieux très spécialisé et, en même temps, vous êtes amené à rechercher ou à exploiter ou faire exploiter des supports numériques au soutien d'investigations dans le domaine de la santé publique. Pouvez-vous nous éclairer sur la manière d'aborder cette question, et l'apport qui peut résulter de ce type de démarche ?

Didier PELTIER.- Je suis magistrat instructeur au pôle santé publique. Mes domaines de prédilection sont l'amiante, l'exercice illégal de la pharmacie ou de la médecine. Cela a bien évidemment peu à voir avec le sujet qui nous occupe.

J'ai pourtant dans mon cabinet trois dossiers qui peuvent illustrer, je crois, le type de dossier que tout magistrat instructeur peut avoir en matière de preuve immatérielle.

Trois exemples permettent peut-être de délimiter le champ d'action du magistrat instructeur.

Il faut rappeler d'un mot que le magistrat instructeur est là pour mettre en état une affaire pénale. Dès lors que la conviction est faite pour le magistrat instructeur que les preuves, que les éléments de charge sont réunis, il va renvoyer le dossier devant une juridiction de jugement. Ce peut être en correctionnelle ou ce peut être la cour d'assises suivant la nature de l'infraction commise (délit ou crime). A travers cette mise en état, à travers cette recherche faite à charge et à décharge, la preuve immatérielle qui est offerte au juge d'instruction est un élément d'investigation extrêmement important.

Trois éléments, trois exemples que je vais décliner tour à tour.

1. La preuve immatérielle comme moyen d'investigation proprement dit

Je travaille particulièrement avec l'OCLCTIC qui fait un travail remarquable, car le travail mené a permis de remonter assez loin dans les investigations. Une grosse société pharmaceutique française a déposé une plainte, car la molécule qu'elle avait nouvellement découverte avait été piratée et elle a constaté, à travers les cellules de veille dont elle dispose au sein de son entreprise, que cette molécule, sous quasiment la même appellation, était vendue sur le Net et était proposée de façon extrêmement générale sur les pays européens, les pays asiatiques d'une façon relativement importante. C'est extrêmement important, extrêmement grave aussi, car un problème de santé publique se pose. Cette nouvelle molécule doit strictement être ordonnée sous prescription médicale et sous surveillance médicale. Le problème est qu'avec la vente libre sur le Net, on n'est pas sûr que cette molécule correspond exactement à la molécule d'origine - il peut y avoir à travers cela des impuretés extrêmement

graves et extrêmement importantes pour la santé publique, et d'autre part, on ne peut en faire un usage sans aucun contrôle médical avec tous les risques que cela comporte.

Nous avons pu travailler en étroite collaboration à travers la plainte qui a été déposée par cette grosse agence pharmaceutique pour, au regard des investigations qui ont été menées par l'Office central de lutte contre la criminalité liée aux techniques de l'information, remonter sur l'ensemble des pays qui desservaient, à travers leur réseau informatique, cette molécule et également sur le pays producteur. Nous avons procédé à des investigations dans quatre pays qui étaient concernés, qui distribuaient cette molécule qui étaient les sites hébergeurs pour les sites qui proposaient la molécule. A travers Eurojust, organe européen qui permet la coordination des opérations de justice et à travers des commissions rogatoires, nous avons pu interpeller des personnes et, pour certaines, des mandats d'arrêt européens ont été délivrés. Une personne a même été détenue en France sur cette base. L'information se poursuit. Nous avons aussi pu, grâce à ces investigations, découvrir quelles étaient, en Chine, les sociétés productrices de cette nouvelle molécule en contrefaçon totale. Nous espérons bien évidemment pouvoir investiguer également sur le territoire chinois pour découvrir la réalité des choses. Vous voyez bien, à travers ces éléments d'information judiciaire, que l'on peut remonter assez loin jusqu'au producteur de la molécule contrefaite et éventuellement interpeller un maximum de personnes - une convention d'entraide internationale a été signée entre la France et la Chine -, et peut-être être les premiers à mettre en œuvre cette convention internationale pour voir extrader certaines personnes vers la France pour être jugées sur ce terrain.

2. La preuve immatérielle comme preuve du lien de causalité

Un ordinateur pose un problème sur le bruit qu'il peut émettre à un moment donné, qui entraîne des acouphènes pour la personne qui l'utilise. Une plainte est déposée par la personne victime de ce dommage, plainte pour blessures involontaires ayant entraîné une incapacité de plus de trois mois, car ce sont des dommages extrêmement importants, et aussi pour mise en danger de la vie d'autrui, car elle vient faire valoir que la société qui commercialise cet ordinateur était parfaitement informée de ce bruit qui pouvait être émis et l'a tout de même mis sur le marché en toute connaissance de cause. Les investigations doivent porter sur : Ce bruit existe-t-il ? Ce bruit existe-t-il, pour le cas où il existe, sur l'ensemble des appareils ? Est-ce que la société qui commercialise cet ordinateur l'a mis sur le marché en toute connaissance de cause ? Il faut aussi, bien sûr, une expertise médicale sur ce terrain pour voir s'il y a un lien de causalité entre le bruit émis et le dommage qui en résulte. La preuve immatérielle joue donc un rôle extrêmement important sur ce domaine.

3. La preuve immatérielle comme élément probant de l'infraction

C'est le cas d'un médecin qui n'hésite pas à faire un exercice illégal de la pharmacie. Il ne se contente pas à son domaine pur médical, mais il joue aussi le rôle de pharmacien en proposant des médicaments *via* un site Internet, son site Internet. Ce médecin propose, à travers un site Internet qui se trouve aux Etats-Unis (le serveur est aux Etats-Unis), des médicaments notamment interdits à la vente sur le territoire national. Les investigations qui seront menées - nous en sommes encore au début de l'information judiciaire - permettront de confondre d'une façon formelle ce médecin à travers la saisie de son ordinateur, à travers l'expertise de cet ordinateur qui permettra de voir que des médicaments sont bien proposés sur ce site et, éventuellement, de le confondre totalement sur ce terrain.

La preuve immatérielle joue donc un rôle extrêmement important pour le magistrat instructeur que je suis, même dans le domaine de la santé publique. Elle est présente

dans tous les domaines, quels qu'ils soient, non seulement dans le domaine financier ou dans le domaine de la pure criminalité, mais également sur un domaine plus pointu qui est celui de la santé publique.

Enfin, lorsque je nomme un expert, je procède comme en matière médicale : j'établis ma mission en totale concertation avec l'expert. Je rejoins ce que disait Alexis RIMBAUD : nous avons chacun un domaine de compétence. Je tiens à avoir ses lumières pour avoir une mission la plus fine possible, la plus précise possible afin qu'elle puisse toucher au plus près de la manifestation de la vérité et éventuellement la faire éclater.

Par ailleurs, le principe du contradictoire existe en matière pénale et au niveau du juge d'instruction désormais. Il a été renforcé avec la loi du 5 mars 2007 dans la mesure où, avant toute mission d'expertise, on doit désormais communiquer notre proposition de mission aux parties. Auparavant, le juge d'instruction signait sa mission et l'envoyait à l'expert. Désormais, le juge d'instruction doit proposer sa mission aux parties, à savoir à la personne qui a déposé une plainte avec constitution de partie civile éventuellement, au plaignant, mais également au mis en examen s'il y en a un, pour le cas où une mission d'investigation et d'expertise intervient à ce moment, et également, bien évidemment, à la partie naturelle qui est le procureur de la République. Ils ont un délai pour faire valoir des observations et ajouter des missions à celles proposées par le juge d'instruction, le juge d'instruction pouvant refuser et, dans ce cas, un débat s'engage qui peut être tranché par la Chambre de l'instruction.

Indépendamment de l'expertise, je considère pour ma part que le juge doit rester maître de son dossier. Alexis RIMBAUD l'a bien dit : l'expert n'est pas un décideur. Le décideur reste le juge sur ce terrain et on doit veiller à ne pas être dépossédé de son dossier à travers une expertise. Pour ma part, j'entends que cette expertise soit suffisamment complète, suffisamment précise, c'est pourquoi je l'élabore en totale concertation avec l'expert qui est missionné, mais aussi qu'elle soit à la portée de tout le monde et qu'elle soit à la portée tant du juge pour qu'il puisse comprendre ce qui est dit et également de la juridiction de jugement qui sera appelée à statuer, *a fortiori* si c'est une cour d'assises comprenant des jurés populaires qui ne sont pas des spécialistes ni, par définition, des magistrats, et qui doivent pour autant comprendre ce qui est dit à travers une expertise. Le juge et la juridiction de jugement ne doivent pas être dépossédés du dossier à travers l'expertise.

M. le Président.- Merci, Didier Peltier. Un vrai dialogue est donc nécessaire entre le juge et l'expert pour construire la mission d'expertise et construire la finalité de l'expertise.

Finalement, dans l'approche de l'expertise, ne faut-il pas anticiper l'expertise dès le début des investigations pour que, y compris dans les hypothèses que vous nous avez présentées, finalement, on puisse sécuriser le support de la preuve pour que, ensuite, son exploitation dans le cadre de l'expertise puisse être satisfaisante ?

Didier PELTIER.- Bien sûr, il faut anticiper au maximum sur ce terrain, prévoir toutes les investigations qui s'avèrent utiles, mais aussi, pour ma part, surtout lorsque l'expertise intervient quasiment *ab initio*. Ils font donc bien évidemment faire en sorte, à travers les premières expertises qui peuvent être diligentées *ab initio*, que les éléments d'une contre-expertise soient sauvegardés. La sauvegarde de tout élément qui sera soumis au principe du contradictoire pur et dur permettra ensuite de faire avancer normalement la procédure.

M. le Président.- Merci pour ces précisions.

Nous arrivons au moment crucial de l'expertise. Serge MIGAYRON, vous êtes experts près des cours d'appel et d'appel administratif de Paris, spécialisé dans le domaine informatique. Comment procédez-vous pour apporter la lumière non seulement aux magistrats qui vous désignent, mais également aux parties concernées par la procédure, plus particulièrement s'agissant de ce que l'on a évoqué tout au long de cette table ronde, de l'intégrité de la preuve numérique et comment, finalement, délivrer un résultat, une information qui soit intelligible, lorsque vous traitez des milliards de données, pour l'ensemble de ces acteurs de la procédure ?

Serge MIGAYRON.- Je voudrais souligner plusieurs caractéristiques de la preuve numérique qui participent à la validité de celle-ci et qui, pour certaines, en sont les conditions nécessaires. J'examinerai successivement l'intégrité, la qualité, l'interprétabilité et l'intelligibilité de la preuve numérique avec tout d'abord l'intégrité de la preuve numérique.

1. L'intégrité de la preuve numérique

L'information numérique a une particularité que tout monde connaît : c'est une information vulnérable. On parle également de malléabilité parce qu'elle est copiable et modifiable avec très peu d'efforts. Il en résulte un risque de non-intégrité, que ce soit par altération ou destruction, volontaire ou accidentelle, et là on a affaire à une information que l'on dit corrompue, qui a été victime de corruption et pour laquelle on ne peut plus garantir son intégrité. Ce risque de non-intégrité de l'information numérique, je voudrais souligner qu'il et présent à chaque stade de la manipulation de l'objet numérique. Ceci dès le scellé judiciaire.

Par exemple, voici un ordinateur portable placé sous scellés. Ne pouvant pas s'ouvrir pour être utilisé, on pourrait assez facilement imaginer que cet ordinateur est protégé dans son intégrité et que l'objet présente des garanties d'intégrité sérieuses. En réalité, en bas à droite du *slide* se trouve une trappe d'accès au disque de l'ordinateur dont on voit, qu'il peut être extrait sans toucher au scellé et donc sans briser le scellé et son intégrité.

Le deuxième niveau de risque dans l'intégrité se pose pour le support de données lui-même. Je citerai le cas de Windows qui est un système dit intrusif. Dès l'instant que l'on utilise Windows pour aller examiner le contenu du disque, qu'on l'ait voulu ou pas, le contenu du disque sera irrémédiablement modifié et le système Windows modifiera ou créera des informations à sa propre initiative qui peuvent être tout à fait subtiles, mais qui auront pour conséquence de pouvoir altérer des preuves que l'on pourrait rechercher. C'est notamment vrai en matière de recherche de fichiers effacés et de datation. Je vous renvoie au n°67 de la revue Experts, pour ceux que cela intéresse, où j'avais développé cette problématique et expliqué quelles étaient les parades.

Enfin, les fichiers et les métafichiers.. En tant qu'expert, on a souvent à examiner des fichiers accompagnés de métafichiers ou de métadonnées, ces derniers étant des informations sur les fichiers. L'exemple le plus simple est celui des propriétés que l'on découvre par le menu "fichier" de documents Office notamment, même celles de droite, qui donnent des dates informatiques, on pourrait penser qu'étant gérées automatiquement par Windows elles apportent un niveau de crédibilité au document sur lequel elles pointent. En réalité, il n'en est rien. Ces informations sont très aisément manipulables et ne peuvent en aucun cas constituer une garantie d'intégrité du fichier concerné. Très rapidement, il est en de même de nombreux autres fichiers, notamment les fichiers d'enregistrement ou fichiers log, qui ont le paradoxe d'être souvent très riches d'informations sur l'état d'un système, mais

comme gros inconvénient d'être extrêmement poreux à toutes les manipulations possibles. Ce sont des fichiers qu'il faut toujours examiner avec beaucoup de réserve.

Les précautions face à ces risques qui sont très nombreux existent et sont de deux ordres :

- Méthodologiques : par une traçabilité très rigoureuse des investigations effectuées, si possible par des mesures visant à assurer la reproductibilité des investigations de manière, en cas de contestation, à ce qu'il soit possible de rejouer un scénario d'investigation sur des bases similaires et sur un protocole d'investigation qui soit également rigoureux, sur lequel les mesures d'investigation puissent s'appuyer.

- Les précautions techniques : elles consistent à ne jamais travailler ou tout au moins éviter de travailler sur un disque original et de faire des copies.

Voici un exemple d'équipements que l'on appelle duplicateurs, qui permet de faire des copies à grande vitesse sur des volumes importants et avec un très haut niveau de sécurité. Il y a malheureusement des cas, lors d'interventions à chaud dans lesquelles un degré d'urgence constitue une contrainte où l'on ne peut pas, où l'on n'a pas le temps de faire des copies et où il est nécessaire de travailler sur un disque original. Dans ce cas on utilise une deuxième catégorie d'équipements que l'on appelle des bloqueurs. Ils permettent d'éviter les inconvénients liés au caractère intrusif de Windows. L'usage de logiciels d'investigation est maintenant très répandu chez les experts, chez les policiers, chez tous ceux qui font de l'investigation. L'intérêt de ces fichiers, indépendamment des fonctionnalités très poussées qu'ils apportent, est de travailler sur des fichiers dits "image", en anglais *evidence file* qui contiennent la totalité, au bit près, de l'information contenue dans un disque dur. A partir de là, on a une très bonne sécurité de ne jamais altérer cette information. S'agissant de la relation entre intégrité et traçabilité, les deux sont pour moi indissociables. Une traçabilité des opérations doit accompagner les mesures qui ont été prises pour garantir l'intégrité d'un support.

2. La qualité

La deuxième caractéristique de la preuve numérique est que l'information dans laquelle elle sera recherchée peut être de qualité très variable. En matière de copie de disque, dans les modalités les plus simples, peut être réalisée sous une forme appelée "copie logique", dans laquelle les fichiers présents sur le disque seront copiés et tout l'espace inutilisé sur le disque sera ignoré. Un deuxième mode de copie est la copie dite physique bit à bit, dans laquelle on copiera l'intégralité du contenu du disque. Ce deuxième mode de copie a déjà un avantage par rapport au précédent : il permettra, le cas échéant, d'aller faire des recherches de fichiers effacés, ce que ne permet pas le premier. Un troisième mode de copie est une copie également physique bit à bit avec une empreinte numérique, on appelle cela une empreinte hash, dont voici un exemple. Ceci est une chaîne de caractères hexadécimaux calculés à partir d'un algorithme MD5 qui garantira que le clone obtenu est strictement identique à l'original. L'intérêt d'une telle signature est qu'un changement, même infime, sur la copie (1 bit) changera radicalement la chaîne de caractères. Il y a donc une extrême sensibilité de cette empreinte à l'information qui se trouve sur le disque. Voilà également un moyen qui permettra de garantir encore un peu plus que la copie obtenue est une copie fidèle de l'original.

En matière de courriel, il y a des tas de façons de sauvegarder du courrier électronique. Dans une façon extrêmement simple, on ne va pas sauvegarder, on ne va pas préserver ce que j'appellerai les "données cachées" qui constituent en réalité le chemin

emprunté par le courriel sur Internet d'un relais à un autre jusqu'à la machine de destination. Suivant le mode de conservation utilisé, ces données seront conservées ou pas. Un niveau de conservation supérieur consistera à conserver non pas un courriel isolé mais à conserver la totalité du fichier de messagerie qu'il contient. L'intérêt de cette mesure est qu'elle permettra, dans certaines conditions, de rechercher des messages effacés, ce qui ne sera naturellement pas possible en conservant les messages individuels. Enfin, on peut encore améliorer la qualité de l'information que l'on veut préserver si l'on conserve le fichier de messagerie dans la globalité, mais également si l'on va sur le serveur rechercher certaines informations, de journaux ou autres qui peuvent venir corroborer ou compléter l'information capturée.

Ces deux exemples sont très simples. Ils ont simplement pour but de vous montrer que les modalités de capture d'une information ou d'un objet numérique seront déterminantes et influeront directement la qualité de l'information dont on va disposer et les possibilités que l'on aura de constituer une preuve numérique valable ou pas.

Je voudrais citer un second élément. Dans le domaine de l'information numérique, il y a un très gros avantage à rechercher un faisceau de preuves. Trop souvent, dans les expertises, on est amené à examiner un objet isolé. Or, l'expérience montre que de disposer d'un faisceau de matériaux ou d'objets numériques, si possible provenant de sources distinctes, contribue de façon considérable à la qualité de l'information et à la preuve que l'on pourra en tirer.

3. L'interprétabilité

C'est une conséquence directe de la malléabilité de l'information. Je citerai quelques exemples pour illustrer la très haute exigence d'interprétabilité que requiert une information numérique.

Face à un courriel sauvegardé dans son fichier de messagerie complet, avec ses données cachées, l'on peut avoir le réflexe de penser qu'il y a toutes les raisons que ce courriel soit intègre. En réalité, c'est une erreur. Avec un peu d'expertise technique, il est très facile d'aller à l'intérieur d'un fichier de messagerie, de viser un message déterminé et de corrompre chacune des informations à volonté de ce message, y compris les informations cachées de routage de ce message. Personne ne sera capable derrière de savoir que ce message a été corrompu. Je parlerai là d'apparence d'intégrité. Cette notion est terriblement dangereuse, dont il faut se méfier.

Un deuxième exemple. Dans la récupération de fichiers effacés, le simple fait, dans un environnement Windows, de supprimer le fichier en le déposant dans la corbeille par exemple aura des effets radicalement différents sur les possibilités de récupération de ce fichier et les outils qu'il faudra utiliser. Un troisième exemple : les analyses de datation évoquées plus tôt. Une date, telle que celle dans les propriétés, est une date calculée sur le fuseau horaire de la machine sur laquelle elle est observée. Ce n'est donc pas une date absolue. Si elle provient d'un scellé saisi dans les DOM-TOM, la date que vous examinerez n'est pas le date à laquelle l'objet a été modifié. C'est bien la date à laquelle vous l'examinez.

L'interprétation est également rendue délicate par une autre caractéristique des technologies aujourd'hui, qui sont des caractéristiques de très grande évolutivité et d'insuffisance d'un point de vue général des spécifications techniques.

La fonction "rechercher" de l'explorateur de Windows, les règles de gestion des dates, de modification de répertoire et de dernier accès à un fichier varient d'une version de

Windows à une autre. Autrement dit, si on a besoin de tirer des interprétations de ces dates, il faut connaître avec certitude la version du système sur lequel les objets ont été prélevés.

4. L'intelligibilité

L'intelligibilité est une condition nécessaire à la validité de la preuve numérique parce que si elle n'est pas intelligible, si elle n'est pas compréhensible, elle ne pourra être exploitée. Les solutions, c'est naturellement les qualités de la rédaction technique. La loi du 5 mars 2007 apporte des dispositions positives, semble-t-il, notamment en autorisant le rapport numérique. Il y a tout à gagner à une mission d'expertise très ciblée plutôt qu'une mission très extensive qui, inévitablement, produira une profusion de matériaux qui rendra plus difficilement intelligible la preuve numérique.

Finalement, il ne faut pas oublier qu'une preuve numérique est une preuve du moment. C'est une preuve en l'état des connaissances. L'algorithme MD5 que j'ai présenté tout à l'heure a déjà été partiellement cassé aujourd'hui et le sera probablement dans les années prochaines. Ce qui est vu aujourd'hui comme une preuve ne le sera donc plus dans quelques années. Ensuite, c'est une preuve très exigeante en rigueur, en méthode, d'outillages et également en compétences techniques multiples. L'article 162 du Code pénal qui autorise aujourd'hui l'expert à se faire aider d'un serviteur dans une spécialité autre que la sienne gagnerait à mon avis une interprétation, dans certains cas, plus souple. Intégrité et qualité, interprétation, intelligibilité sont bien les conditions de validité de la preuve numérique et donc de la sécurité de l'expertise numérique. Sur l'intelligibilité, je terminerai par un mot : une preuve numérique, il ne faut pas oublier qu'elle peut ne pas être certaine. On peut être dans des domaines où il est nécessaire d'avoir recours à l'appréciation ou à la corroboration. Une preuve numérique peut ne pas être binaire. Merci.

M. le Président.- Merci, Serge Migayron.

Face à l'ampleur du cauchemar que nous ont révélé Laurence IFRAH et Alain BENSOUSSAN, et pour assurer la prospérité du travail des enquêteurs comme cela nous a été évoqué, l'expert doit permettre d'apporter un éclairage à la fois sur l'analyse de l'information - c'est le résultat de l'expertise -, mais aussi sur la garantie, sous le contrôle du juge, de la qualité de l'information traitée. Vous avez pu voir au travers des différentes interventions tout l'intérêt de la réflexion sur le travail de l'expertise et donc, effectivement, l'intérêt de l'ouvrage que nous a produit Alexis RIMBAUD.

Echanges avec l'auditoire

Jacqueline DERAY, informaticienne.- Je voudrais confirmer un point. En 1986, déjà, les statistiques de l'APSAIRD donnaient dans la criminalité informatique les deux tiers des victimes pour être les assureurs et les banquiers. C'est ce fait qui explique le silence et la confidentialité parce que les banquiers comme les assureurs vivent de leur image de marque et de la sécurité. D'où le fait que les grandes affaires que l'on pourrait imaginer ne sont jamais évoquées et ce sont finalement plutôt les simples particuliers délinquants qui sont aujourd'hui la clientèle courante.

M. le Président.- Merci, madame. Des préjudices sont colossaux au niveau international. Il y a un problème de réponse pénale à ces phénomènes.

Fabien LANG.- Vous avez raison, madame. Je n'ai pas connaissance d'actes frauduleux qui auraient visé les assureurs. Mais il est évident que les grandes banques - notamment sur des affaires importantes de *fishing* internationales qui visaient la captation de données permettant aux fraudeurs de s'insérer dans les comptes bancaires en ligne des particuliers et de procéder à des virements - étaient toutes visées par ces phénomènes, et pas seulement en France. Ces dernières ont eu beaucoup de difficulté à révéler ces affaires parce que nous connaissons une phase de développement économique très importante en matière de banque en ligne et qu'il ne fallait absolument pas révéler ce type de faille. Pour ces affaires d'ailleurs, ce n'étaient pas les banques qui étaient spécialement visées mais les particuliers.

La problématique concerne actuellement la protection des ordinateurs particuliers. Les fraudeurs ne s'attaquent pas ou très rarement, pour le moment en tout cas, aux bases de données d'établissements bancaires ou de grandes sociétés qui sont relativement bien protégées. Ils s'attaqueront à des particuliers qui ne connaissent pas forcément ou qui n'ont pas nécessairement envie non plus de se protéger, de mettre à jour leur antivirus, de mettre à jour leur système de d'exploitation. La vulnérabilité se trouve donc aujourd'hui à ce niveau. Encore une fois, les risques sont importants. En France, nous sommes encore relativement bien protégés par notre système bancaire, notamment de transactions par carte bancaire qui oblige les commerçants à transmettre assez rapidement les données recueillies dans le cadre de ces transactions à leur établissement bancaire. Cela risque d'évoluer avec les directives européennes qui vont totalement libéraliser ce type de transactions. Ce n'est pas le cas dans des pays comme les Etats-Unis notamment où ce sont des intermédiaires, des acquéreurs privés qui peuvent procéder à ce type d'activité et procéder aux transactions à la place des banquiers, ce qui a occasionné et qui occasionne très régulièrement des actes de piratage extrêmement importants. L'affaire TGX concerne un gros commerçant américain représenté sur tout le territoire américain et qui a été victime du vol de plusieurs dizaines de millions de numéros de cartes bancaires. Ces numéros se trouvent actuellement sur Internet, sur des forums, des marchés noirs qui vont maintenant s'efforcer de revendre ces numéros en gros, en demi-gros sur ces marchés internationaux. Les risques sont effectivement importants, mais ces établissements n'ont pas forcément envie de le faire savoir.

M. le Président.- Merci.

Eric FREYSSINET, gendarmerie nationale.- La présentation de M. BENSOUSSAN pouvait laisser croire que l'on traitait peu de preuves numériques au bout du compte, mais la réalité est aujourd'hui qu'énormément d'affaires nécessitent de traiter des supports de preuve numérique, donc pas uniquement les infractions spécifiques. Je pense que ce n'était pas le but de son intervention. Cela veut dire aussi que les experts ne sont pas les seuls à être amenés à traiter ces supports de preuve. La moindre enquête judiciaire au pénal aujourd'hui touche des téléphones portables, peut-être l'utilisation d'Internet. Il faut donc traiter ces supports, dès le départ avec toutes les précautions nécessaires. L'enquêteur procède à la perquisition souvent sans expert, mais en revanche de plus en plus avec des enquêteurs spécialisés.

Le deuxième point porte sur les méthodes. D'une part, dans les laboratoires d'expertise et dans les cabinets d'expertise, on développe depuis plusieurs années des procédures écrites documentées. C'est une démarche d'assurance qualité. Dans les laboratoires, cela se traduit par des démarches d'accréditation. La gendarmerie a entrepris l'accréditation au titre de la norme ISO 17025 qui réglemente le travail dans les laboratoires d'expertise. Ce sera très bientôt le cas pour le département qui s'occupe d'informatique, mais c'est déjà le cas pour les véhicules, les documents, et ce sera très bientôt le cas pour l'ADN puisque la législation nous y contraindra, etc.

Cette démarche est déjà bien entreprise. Au-delà de cela, se pose le problème de la publication des méthodes. L'accréditation en France ne nécessite pas la publication, mais nécessite que les méthodes soient documentées et disponibles pour notamment les services chargés de l'accréditation. Madame IFRAH évoquait l'*anti-forensic*. Publier les méthodes, les rendre disponibles par exemple intégralement dans les rapports d'expertise et donc disponibles auprès des fraudeurs que l'on poursuit pourrait mettre à mal quantité de notre travail. Il faut donc trouver un bon équilibre. Pour nous, l'équilibre est au travers de la transparence. Les méthodes existent, elles sont documentées. S'il doit y avoir une contre-expertise, elles seront présentées aux contre-experts, etc. Ce sont des choses déjà bien possibles, mais avec le bémol que j'évoquais. La publicité des faits est un grand problème. Il y a peu d'affaires, mais il y en a. Il existe même des affaires de piratage assez importantes en France. On en parle assez peu parce que, services d'enquête et magistrats, nous sommes très soucieux de conserver une certaine confidentialité sur les affaires sensibles. Toutefois, le procès pénal est public. Au moment du procès, il existe donc le risque que le nom de l'entreprise victime soit dévoilé, etc. Cela peut poser des difficultés.

Il existe deux points de vue. La possibilité évoquée la semaine dernière à la Commission européenne d'avoir des victimes sous x aurait un mauvais effet, car cela éviterait l'effet pédagogique de la position de victime puisqu'il n'y aurait plus de crainte à mal protéger son système. Je crois plus à la nécessité d'une préparation de l'entreprise, des administrations, de toux ceux qui gèrent des systèmes d'information à la possibilité d'une crise, c'est-à-dire d'une atteinte à leur système d'information et qu'elles soient en mesure de porter plainte et préparées à communiquer sur ce dépôt de plainte éventuellement.

M. le Président.- Merci, Eric Freyssinet. Une réaction, peut-être ; Alexis Rimbaud, puisque vous avez parlé de certification ?

Alexis RIMBAUD.- La certification devient presque obligatoire dans le cadre de l'expertise. Pour reprendre le contexte que vous avez évoqué, on a effectivement en provenance certains d'éléments aussi bien de la part des OPJ que des magistrats, et le travail est partagé. A tel point que le travail de l'expert, le travail de la source de la preuve numérique

est en train changer. On est de plus en plus contraint à un traitement le plus rapide possible de l'affaire, presque à une immédiateté. Je me suis livré à quelques calculs pour savoir où se situait véritablement le temps de traitement puisque cela a souvent fait l'objet de plaintes de justiciables qui se plaignaient du temps de traitement de l'expertise. C'est aussi un problème. L'expert travaille. Il génère de la preuve, mais il travaille souvent lentement et prend beaucoup de temps. Il est vrai qu'il vient en opposition à ce mouvement global d'immédiateté de l'information et il s'oppose souvent à cette volonté d'immédiateté de réponse. Pour vous donner un ordre d'idée, j'ai classé les temps de traitement, et ces chiffres parlent d'eux-mêmes, sur les mécanismes actuellement en train de se mettre en place, par exemple la LOLF qui administre l'expertise, qui administre aussi la preuve indirectement.

Je reçois dans mon laboratoire deux types de demandes : des demandes de la part des OPJ sous forme de réquisitions et des demandes d'expertise de la part des magistrats. Pour les réquisitions par exemple, le temps de traitement de devisage, de validation LOLF, c'est-à-dire du retour du parquet, de la récupération des éléments à expertiser, cette partie prend 6 jours. L'opération expertale elle-même prend 9 jours. Ce sont des moyennes. Le temps de traitement global en réquisition est donc de 15 jours et le pourcentage d'administration sur le temps total de 66 %. Le travail de l'expert, le temps pris par l'expert est occupé à 66 % par l'administration. Dans le cadre de l'expertise, le temps consacré à la récupération des éléments expertisés, du rapport avec le magistrat, de la gestion, de la pré expertise, du devisage et de la validation LOLF (étant entendu que l'on n'est même pas encore au début de l'expertise, du travail expertal) prend en tout 19 jours. L'opération expertale elle-même prend en moyenne 31 jours. Cela fait 47 jours de traitement au total, soit 25 % du temps global attribué au travail de l'expert.

Cela signifie, si l'on veut aller beaucoup plus vite dans le temps de traitement de la preuve numérique, qu'il faudra aussi augmenter les systèmes de gestion de la preuve et plus globalement les systèmes mis à la disposition des magistrats et de la loi.

M. le Président.- Merci pour ces précisions. Effectivement, à travers la LOLF, le juge devient un ordonnateur de dépenses et il doit donc administrer le coût. Le déroulement des opérations peut avoir une incidence sur le résultat. D'autres remarques ?

Un intervenant.- Des contre-exemples flagrants existent où le juge d'instruction est allé très vite pour nous confier des scellés. Je me souviens d'un dossier où quatre personnes étaient incarcérées et il fallait aller vite. Entre le moment où j'ai été appelé et le moment où j'ai remis mon rapport d'expertise, quatre jours ont passé. Je me souviens même avoir fait des copies des scellés directement dans le service de police..

M. le Président.- C'est une contrainte croissante. Je crois que nous avons épuisé notre temps. Merci de votre attention.

Michel ROUGER.- C'est la fin d'un colloque qui fut passionnant, grâce à ceux qui l'ont animé. Nous l'avons imaginé à quatre : Thomas CASSUTO, Alexis RIMBAUD, Michel ARMAND-PREVOST et moi. Quand il s'est agi de le monter, nous avons eu quelque peine à faire comprendre ce que nous voulions faire. Nous y avons été bien aidés par Maître FERAL SCHUL.

Le procès, depuis le juge Bridoye, cher à Rabelais, est tellement dépendant des sacs et des sacoches de papiers, de l'assignation à la grosse du jugement, que nos interlocuteurs faisaient les yeux ronds quand on leur parlait de preuves immatérielles. Dans le

procès pénal, qui repose de plus en plus sur les travaux des experts, de Manhattan à la télé, ou de la rue des Italiens à Paris, l'intérêt a été plus vif.

Toutefois, il s'est cantonné à la procédure d'expertise, dans un débat d'initiés, entre l'expertise contradictoire en matière civile et rendue contradictoire en matière pénale. Nous voulions faire la différence entre les deux procédures lorsque l'expertise s'y engage. Nous y sommes arrivés en organisant deux tables rondes.

Chacune des deux est restée dans le concret.

Dans la première, toutes les parties prenantes à l'expertise en matière civile ont bien décrit et commenté l'intrusion de l'immatériel dans les prétoires, chez le juge, l'avocat, l'expert, l'huissier de justice.

Dans la seconde, la vision s'est élargie au-delà des praticiens du procès pénal pour aller vers le chercheur qui explique les phénomènes et le policier qui précède ou suit le juge, l'expert et l'avocat dans l'enquête.

L'ouvrage d'Alexis RIMBAUD a éclairé, de manière crue et réaliste, les activités du quotidien de ces techniciens de l'immatériel, qui développent leurs prestations au service des juridictions répressives.

Nous voulions marquer la différence de pédagogie entre la table ronde civile et la table ronde pénale. L'arrivée des éléments de preuve immatérielle dans le procès civil ne le perturbe pas. Dans le pénal, l'élément immatériel trouble le jeu. Il y crée de l'insécurité en rendant le travail du juge, de l'expert et de l'avocat extrêmement compliqué. C'est pourquoi nous souhaitions ouvrir un débat. Nous voulions le faire ici parce la Maison du barreau est bien l'endroit où ces choses peuvent y être le mieux traitées. Vous en recevrez les conclusions ou vous les trouverez sur le site PRESAJE.

Grand merci à vous tous.

(Applaudissements.)

Les débats sont clos à 18 heures 15.