

COMPAGNIE NATIONALE DES EXPERTS DE JUSTICE
EN INFORMATIQUE ET TECHNIQUES ASSOCIEES



Colloque du 13 Avril 2010

à la Première Chambre de la COUR d'APPEL de PARIS

La preuve numérique à l'épreuve du litige

*Les acteurs du litige face à la preuve numérique
(l'information numérique fait la preuve)*

SOMMAIRE

I. Ouverture du Colloque	5
Monsieur Patrick MATET : Président de la 1ère Chambre, Pôle 1, de la Cour d'Appel de Paris	5
Monsieur Nathan HATTAB : Président de la Compagnie Nationale des Experts de Justice en Informatique et Techniques Associées.....	8
II. De l'information numérique à la preuve numérique	9
II.1. <i>Définitions et cadre juridique de la preuve numérique</i> Madame Mélanie CLEMENT-FONTAINE, Maître de Conférences, Co-directeur du master NTIC Université de Versailles Saint Quentin en Yvelines, Membre du Laboratoire Dante	9
II.2. <i>Critères d'appréciation technique, vraies et fausses preuves numériques</i> Monsieur Serge MIGAYRON : Expert de Justice près la Cour d'Appel de Paris.....	19
III. Constituer une preuve numérique.....	29
III.1. <i>Introduction</i> Monsieur Vincent VIGNEAU : Conseiller référendaire à la Cour de Cassation, Professeur associé à l'Université de Versailles Saint Quentin en Yvelines – Membre du Laboratoire Dante	29
III.2. <i>L'huissier collecteur de preuve numérique volatile</i> Maître Jérôme LEGRAIN : Huissier de Justice associé à Paris	35
III.3. <i>Police judiciaire et nouveaux territoires de l'information numérique</i> Monsieur Christian AGHROUM : Chef de l'OCLCTIC	40
III.4. <i>L'avocat ensemblier de preuves numériques</i> Maître Olivier ITEANU : Avocat à la Cour.....	43
III.5. <i>L'expert et les bonnes pratiques techniques</i> Monsieur David BILLARD : Expert de Justice près la Cour d'Appel de Chambéry	47
III.6 <i>Débat avec la salle.....</i>	50

IV. Exploiter une preuve numérique	56
IV.1. <i>Introduction</i>	
Monsieur Nathan HATTAB : Président de la CNEJITA	56
IV.2. <i>Le Juge pénal, ses attentes, une preuve sûre et intelligible</i>	
Monsieur David BENICHOU : Vice Président en charge de l'Instruction au Tribunal de Grande Instance de Nanterre	57
IV.3. <i>Exemples de difficultés rencontrées par le Juge chargé du Contrôle des Expertises</i>	
Monsieur Jean-Pierre LUCQUIN : Juge consulaire, Délégué Général au Tribunal de Commerce de Paris	63
IV.4. <i>La dissymétrie de la charge de la preuve et coût</i>	
Maître François-Pierre LANI : Avocat à la Cour.....	67
IV.5. <i>La dynamique de la preuve numérique dans l'expertise</i>	
Monsieur David ZNATY : Président de la Compagnie des Experts agrés par la Cour de Cassation	73
IV.6. <i>Débat avec la salle</i>	76
V. Clôture du Colloque.....	81
V.1. <i>Synthèse et perspectives</i>	
Madame Mélanie CLEMENT-FONTAINE, Maître de Conférences, Co- directeur du master NTIC Université de Versailles Saint Quentin en Yvelines, Membre du Laboratoire Dante	81
V.2. <i>Clôture des travaux</i>	
Monsieur Nathan HATTAB, Président de la CNEJITA :	86

I. Ouverture du Colloque

Monsieur Patrick MATET : Président de la 1^{ère} Chambre, Pôle 1, de la Cour d'Appel de Paris

Je me réjouis de vous accueillir dans ce lieu, symbolique où tant de procès retentissants se sont déroulés. Le contraste est saisissant entre ce lieu qui témoigne de la permanence de la justice et le sujet d'une actualité brûlante que vous avez choisi pour ce colloque. Avec l'avènement de l'ère du numérique et de la révolution numérique, l'information et la communication se sont accélérés et simplifiés. Chacun d'entre nous serait devenu un *homo numericus*, selon l'expression consacrée et employée par les auteurs d'un savant rapport remis au Sénat. Comme nous le savons tous, nos activités laissent des traces enregistrées et conservées. Même si nous n'en avons qu'une conscience diffuse, nos activités sont suivies par les caméras de vidéosurveillance, par les téléphones portables, par les cartes bancaires, par les cartes de transport en commun, par Internet... Depuis les années 2000, l'écrit sous forme électronique est admis en preuve en droit civil comme en droit pénal. Pourquoi alors consacrer un colloque à la question subtile de la preuve numérique à l'épreuve du litige ? Dans un procès, des questions de fait et de droit doivent être tranchés. Quand ces questions sont complexes, l'administration de la preuve requiert le plus souvent le recours à l'expertise judiciaire. Or l'expertise judiciaire est multiple dans la mesure où elle est régie, selon le cas, par les règles de procédure civile, de procédure pénale ou de procédure administrative et qu'à ces règles générales s'ajoutent des spécificités liées à certaines expertises particulières, comme les expertises immobilières, financières ou de responsabilité médicale. Je crois qu'il convient d'ajouter à cette liste non exhaustive l'expertise numérique.

Dans le maquis du droit de la preuve, je discerne un trait saillant de la preuve numérique : elle entre souvent en tension avec d'autres droits de nature différente, notamment les libertés publiques. Fréquemment, une des parties à l'expertise diligentée dans le cadre de la preuve numérique opposera au recueil des données informatiques le droit à la vie privée, au secret des correspondances ou au secret des affaires. Certes la justice est souvent confrontée à ces choix antagonistes entre preuve et liberté mais la question devient réellement aigüe avec la preuve numérique. Le fait que le Sénat ait récemment adopté une proposition de loi visant à mieux garantir le droit à la vie privée à l'heure du numérique, en mettant en avant un nouveau droit à l'oubli illustre bien l'existence d'une confrontation entre droits de nature différente.

Par ailleurs, la fugacité des données informatiques et numériques multiplie les difficultés de recueil et de conservation de la preuve et la nature immatérielle de ces données entraîne un effacement problématique des frontières entre sphère privée et sphère professionnelle notamment dans l'activité des salariés. Cette nature immatérielle oblige aussi à reconsidérer les notions de souveraineté étatique, face à l'extraterritorialité des données qui ne sont pas toujours constituées dans le pays de commission de l'infraction : la cybercriminalité s'épanouit dans des réseaux numériques complexes et pose des questions juridiques nouvelles pour les pénalistes.

Confrontés à toutes ces difficultés, nous pourrions être tentés de conclure que le droit s'épuise à poursuivre la preuve numérique dont les frontières s'échappent toujours plus loin. La justice est-elle condamnée, comme Sisyphe, à faire un travail inutile et vain en matière de preuve ? Sur ce point, nous pouvons affirmer que la preuve numérique est effectivement en perpétuelle construction et que, même si elle s'élabore moins rapidement que la technique qui évolue à grande vitesse, le cadre juridique de la preuve numérique dans le litige est le droit de la preuve. Or, les attentes des justiciables, des avocats et des juges sont les mêmes pour la preuve numérique et les autres preuves : cette preuve doit être fiable et crédible. Pour que la preuve numérique soit

fiable, ou solide comme disent les Anglo-saxons à propos de l'admissibilité de la preuve recueillie lors de la *discovery*, il est impératif que les données soient réunies selon une méthodologie acceptée par tous. Pour qu'elle soit crédible, elle doit résister à la discussion : l'expert doit alors tout mettre en œuvre pour que les parties puissent débattre de toutes les questions posées par cette preuve numérique. La convention signée en 2009 par la Cour d'appel de Paris, les barreaux des neuf tribunaux du ressort et l'Union des compagnies d'experts près la cour d'appel de Paris demande aux experts de remettre aux parties un document de synthèse avant qu'elles n'émettent leurs observations, afin de favoriser la discussion et épuiser le débat technique lors du temps de l'expertise. C'est à l'aune de cette discussion contradictoire que le juge se convaincra de la pertinence des conclusions expertales. Les débats de cet après-midi feront progresser notre réflexion et je remercie tous ceux qui vont œuvrer en ce sens. Sur ces questions techniques, n'est-ce pas le propre des experts, comme le dit l'article 232 du Code de procédure civile, d'apporter à la Justice ces lumières ?

Monsieur Nathan HATTAB : Président de la Compagnie Nationale des Experts de Justice en Informatique et Techniques Associées

J'ai le plaisir de vous accueillir dans ce colloque de la Compagnie Nationale des Experts de Justice en Informatique et Techniques Associées pour une réflexion sur le thème de la preuve numérique à l'épreuve du litige.

Je remercie le Premier Président de la cour d'appel de Paris d'avoir accepté de nous accueillir dans cette superbe salle ainsi que le laboratoire DANTE de l'université de Versailles Saint-Quentin en Yvelines pour sa contribution à ce colloque.

Lorsque les experts sont amenés à expertiser un objet comportant des éléments d'information numérique, ils se posent de nombreuses questions, notamment sur le processus de collecte de ces informations, sur leur conservation, sur les vérifications et sur les précautions à prendre. Ce colloque voudrait répondre au moins en partie à ces questions. Il est organisé en quatre étapes avec une présentation du cadre juridique de la preuve et des critères d'appréciation de la preuve numérique puis deux tables rondes consacrées respectivement à la constitution de la preuve numérique et à l'exploitation de la preuve numérique. Enfin, nous terminerons ce colloque par une synthèse.

La Compagnie nationale des experts de justice en informatique et techniques associées (CNEJITA) dispose d'un site (www.cnejita.org) sur lequel vous pourrez trouver les actes du colloque de l'année dernière et ceux de cette année.

II. De l'information numérique à la preuve numérique

II.1. Définitions et cadre juridique de la preuve numérique

Madame Mélanie CLEMENT-FONTAINE, Maître
de Conférences, Co-directeur du master NTIC
Université de Versailles Saint Quentin en Yvelines,
Membre du Laboratoire Dante

Je tiens à remercier les membres de la Compagnie Nationale des Experts de Justice en Informatique et Techniques Associées de m'avoir invitée à ce colloque consacré à la preuve numérique.

En 1829, Domat définissait la preuve comme suit : « on appelle preuve ce qui persuade l'esprit d'une vérité (...). On appelle preuves en justice les manières réglées par les lois pour découvrir et pour établir la vérité d'un fait contesté ». A travers cette définition, Domat nous invite à appréhender la notion de preuve selon deux angles distincts : d'un point de vu général, la preuve permet d'établir la vérité ou du moins persuader l'esprit d'une vérité ; du point de vu juridique, les preuves sont des

mécanismes encadrés par la loi permettant de rendre opératoire un droit ou d'établir une culpabilité. Les preuves sont, par conséquent, indispensables à l'effectivité d'un droit : c'est pourquoi elles répondent à des règles précises.

Avec le développement des moyens d'investigation (tant numérique que biologique ou biotechnologique), l'exigence de vérité semble plus pressante. Le droit s'adapte pour accueillir ces modes de preuve tout en gardant une distance avec le présupposé du tout scientifique. D'ailleurs, la recherche de vérité en droit n'a jamais été absolue : en témoigne le mécanisme de la présomption qui consiste à partir d'un fait connu pour en déduire un fait inconnu ou encore celui de la fiction qui permet pour tenir comme exact un fait qui ne l'est pas forcément. Il est en effet parfois préférable, dans un souci d'ordre social, de faire prévaloir la vraisemblance sur la vérité.

La conception juridique de la preuve ne se confond pas avec une conception scientifique de la preuve. Par exemple, pour des questions d'éthique, le respect dû aux morts fera obstacle à l'exhumation d'un corps afin d'établir une filiation entre le requérant et le défunt si ce dernier n'a pas exprimé son accord avant sa mort. Bien que la science permette d'établir une vérité (le lien ou l'absence de lien de filiation), le législateur entend établir des limites résultant d'une recherche d'équilibre entre des impératifs contraires.

Ainsi, il est possible d'affirmer que l'établissement de la vérité n'est pas l'unique objectif recherché mais qu'il doit être concilié notamment avec le respect des libertés fondamentales, le respect de la vie privée et d'autres droits. En somme, la collecte de la preuve répond à deux principes : le principe de loyauté et celui de proportionnalité. Ces règles ont pour objet de déterminer

qui doit établir la preuve, sur quoi doit porter la preuve, comment elle doit être établie et quelle est sa force probante. Classiquement, l'étude du droit de la preuve se présente en trois points : la charge, l'objet et le mode de preuve. Selon le domaine considéré (pénal, civil, administratif), les règles divergent. Par exemple, en droit pénal la preuve est en principe libre ce qui offre la possibilité aux parties d'avoir recours à toutes les modalités permettant d'établir la vérité. Au contraire, en droit civil, tantôt la preuve est libre, tantôt il y a un *numerus clausus* qui impose des moyens de preuve limitativement énumérés par la loi. Dans ce contexte, la preuve numérique n'est pas appréhendée de la même manière selon les cas.

La preuve numérique est une modalité particulière d'établissement de la vérité qui consiste à avoir recours à des moyens numériques variés qui vont de l'étude des contenus dans la mémoire d'un disque dur, aux messages électroniques, en passant par l'enregistrement numérique. Quand la preuve est libre, la preuve numérique a pu se développer rapidement. Inversement, lorsque l'écrit est le mode de preuve exigé comme en droit civil, il a fallu attendre l'intervention du législateur pour ouvrir la preuve au champ du numérique. L'écrit ayant longtemps été admis uniquement sur support papier, il a fallu reconnaître qu'il puisse être également sur support numérique. L'initiative du législateur était nécessaire, sinon indispensable, à l'heure où les moyens d'échange, de stockage, de production sont majoritairement numériques.

Pour autant, le caractère immatériel, volatile et évolutif de l'information numérique sont autant d'obstacles à son élévation au rang de preuve. La preuve numérique suppose la maîtrise d'outils numériques en perpétuelle évolution sans que personne n'ait beaucoup de recul face à leurs usages. La place de l'expert

devient alors déterminante. En outre, l'obtention de la preuve numérique conduit à trancher des questions juridiquement déterminantes comme celle de la frontière entre sphère privée et sphère publique partiellement brouillée dans un monde numérique. L'issue de la réponse commande pourtant la validité de l'obtention de la preuve.

La lecture des lois donnent une fausse impression de simplicité : lorsque la preuve est libre, la preuve numérique peut prospérer, et quand bien même la preuve doit être faite par écrit, ce dernier, depuis la loi de 2000, peut être sur support papier ou numérique. Or, sous cette apparente simplicité, les choses se compliquent. D'une part, celui qui aura la charge de la preuve, face aux difficultés techniques, se tournera vers les experts. In fine, le juge devra apprécier la recevabilité des preuves fournies et déterminer leur force probante. La tâche pourra être délicate dans un domaine où il ne maîtrise pas forcément toutes les techniques en évolution. Le juge a toutefois la possibilité de désigner un expert si cela lui paraît nécessaire. Il peut également enjoindre une partie à produire des éléments de preuve. Compte tenu de l'évolution des techniques, le juge doit affiner son appréciation de la légalité de l'établissement de la preuve. Régulièrement il doit se prononcer sur de nouveaux cas de figure. De l'apparence simplicité de la reconnaissance juridique de la preuve numérique, il résulte de l'étude de la jurisprudence une complexité non négligeable liée à la preuve numérique.

L'apparente simplicité de la preuve numérique

Le droit de la preuve est un domaine qui a connu des mutations profondes. Du temps de la justice sacrée jusqu'au XIII^{ème} siècle en Europe, les modes de preuves ont un caractère irrationnel et religieux difficilement concevable aujourd'hui, parmi

lesquels on retiendra l'épreuve de l'eau ou du feu ou encore du duel judiciaire. A partir du XIII^{ème} siècle, s'opère un passage de l'irrationnel au rationnel avec un système de preuve très hiérarchique. Le fait notoire ou la règle notoire est supérieur aux preuves pleines qui sont établies par un double témoignage ou un acte authentique, qui sont à leur tour supérieures aux preuves semi-pleines. Le deuxième changement notable date du XIV^{ème} siècle lorsque la preuve écrite devient la preuve par excellence supplantant la preuve orale. Cette rupture n'est pas le fruit d'une amélioration quant à l'obtention de la vérité mais une affaire de circonstances. Elle tient à l'exigence, dans le procès, de rapidité et de simplicité. La troisième rupture qui nous intéresse est celle de la reconnaissance de la preuve numérique par la loi du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique. Il a été souligné le rapprochement entre les deux dernières mutations : chacune de ces mutations n'ont pas tant été guidées par les qualités probatoires intrinsèques de l'écrit (papier puis numérique) mais par la volonté de simplifier le règlement des conflits.

Le retard numérique de la France fut remarqué dans les années 1990 puisque 20 % des français avaient alors accès à Internet, contre une moyenne européenne de 36 %. Il était donc indispensable de redresser la situation. Une des premières préoccupations a été de définir les modalités de la collecte des preuves dans l'environnement numérique. En 1995, le Conseil de l'Europe a rendu une recommandation afin que les Etats créent des unités spécialisées pour la répression des infractions. Il existe en France plusieurs établissements publics (Institut de recherche criminelle de la gendarmerie nationale, la brigade d'enquête sur les fraudes aux technologies de l'information...) ou privés (comme l'Agence pour la protection des programmes ou les sociétés de gestion collective). Tous contribuent à la collecte de la preuve.

La démarche du législateur a été bien souvent guidée par l'idée de neutralité juridique. En effet, la loi du 13 mars 2000 tend à effacer toute référence au support de la preuve littérale qui peut dès lors être numérique ou papier. L'article 1316 du Code civil dispose désormais que « la preuve littérale, ou preuve par 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 leurs modalités de transmission ». L'efficacité de la preuve est depuis soumise à deux exigences exposées à l'article 1316 du Code civil qui sont d'une part que la personne soit dûment identifiée et d'autre part que le document soit conservé et que cette conservation soit garante de son intégrité. Selon le principe de la neutralité technologique, aucune distinction n'est faite entre l'écrit papier et l'écrit électronique. Il est par ailleurs affirmé à l'article 1316-3 du Code civil que "l'écrit sur support électronique a la même force probante que l'écrit sur support papier".

Cette évolution de la notion d'écrit en tant que preuve nécessitait comme corollaire une reconnaissance juridique de la signature électronique. Tel a été également l'objet de la loi du 13 mars 2000 qui transpose la directive du 13 décembre 1999 relative à la signature électronique. Il en résulte l'article 1316-4 du Code civil qui définit la signature électronique comme « l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache ».

En outre, il est possible d'aménager contractuellement les modalités de preuve. Dans ce cas, les parties décident ensemble des procédés autorisés de preuve pour justifier leurs droits. Cette possibilité est ouverte alors même que la preuve doit être faite en principe par écrit. En effet, l'article 1341 du Code civil n'est pas d'ordre public. Les conventions de preuve sont particulièrement

utiles en matière de commerce électronique et de monnaie électronique. Par exemple, les contrats portant sur les cartes bleues stipulent habituellement que « les enregistrements des appareils automatiques ou leur reproduction sur support informatique constituent pour l'établissement émetteur la preuve de l'opération effectuée au moyen de la carte et justifie l'imputation du compte ».

Ce rapide rappel des principes qui gouvernent la preuve numérique conduit à s'interroger sur leur mise en œuvre. Il en résulte que le caractère immatériel, volatile, évolutif de l'information numérique fragilise la portée de la preuve numérique.

La complexité avérée de la preuve numérique

La preuve numérique est soumise à des deux séries d'exigences juridiques. Sa collecte doit être loyale et proportionnée. Lorsqu'elle a pour objet un acte, sa recevabilité est conditionnée à des exigences d'intégrité, d'imputabilité et de fiabilité.

A. La collecte : les principes de loyauté et de proportionnalité

Les principes de loyauté et de proportionnalité dans la collecte des preuves numériques n'ont pas la même portée selon les domaines concernés.

Le principe de loyauté

En matière sociale par exemple, un litige concernait la preuve constituée à partir de vidéosurveillance. Dans une affaire récente, un système de vidéo surveillance avait été mis en place par un employeur afin de surveiller la clientèle et les vols. Un

employé a été pris sur le fait alors qu'il volait dans le magasin. L'employeur a donc constitué cette preuve à partir de la vidéosurveillance et l'employé s'est opposé à cette preuve en faisant valoir qu'elle était contraire au principe de loyauté puisque le système de surveillance n'avait pas pour objectif de surveiller les employés et portait par conséquent atteinte à sa vie privée. Les juges de la cour d'appel de Bourges ont dans un premier temps jugé recevable la production d'un enregistrement du salarié effectué par l'employeur, « estimant qu'il ne pouvait être sérieusement prétendu que le salarié ignorait l'existence de caméras vidéo destinées à détecter les vols perpétrés dans l'entreprise et utilisées depuis 1996 ainsi qu'il ressort de la consultation du CHSCT produite par l'employeur et annoncée par des affichettes dans le magasin ». Cette décision a cependant été sanctionnée par la chambre sociale de la Cour de cassation, le 7 juin 2006, pour violation de la loi car, selon l'attendu de principe « si l'employeur a le droit de contrôler et de surveiller l'activité de son personnel durant le temps de travail, il ne peut mettre en œuvre un dispositif de contrôle qui n'a pas fait l'objet, préalablement à son introduction, d'une information et d'une consultation du comité d'entreprise ». La collecte de preuve numérique nécessite donc une certaine publicité des moyens mis en œuvre pour être considérée comme loyale.

Par contre, en droit pénal, l'exigence de loyauté est moins forte. Ainsi, dans une affaire d'abus de bien sociaux, la preuve de l'infraction avait été apportée au moyen d'un enregistrement d'une caméra de surveillance. La défense faisait valoir que l'enregistrement avait été fait à l'insu des salariés et par conséquent avait porté atteinte à l'intimité de leur vie privée. La Chambre sociale de la Cour de cassation, par un arrêt du 6 avril 1994, rejette le pourvoi en précisant que « aucune disposition légale ne permet aux juges répressifs d'écarter les moyens de

preuve produits par les parties au seul motif qu'ils auraient été obtenus de façon illicite ou déloyale ; qu'il leur appartient seulement, en application de l'article 427 du Code de procédure pénale, d'en apprécier la valeur probante ». L'établissement de la commission d'une infraction à partir de preuve numérique est ainsi facilité. Seule l'incitation à commettre les infractions en constitue la limite. Nonobstant cette limite, depuis la loi du 5 mars 2007, il est prévu à l'article 706-35-1 du Code de procédure pénale que la police judiciaire est autorisée à procéder à des infiltrations numériques dans le but de constater des infractions..

Le principe de proportionnalité

La collecte de preuves numériques peut conduire à porter atteinte aux libertés individuelles ou collectives des personnes. Il doit donc être opéré un équilibre entre la légitimité de pouvoir se constituer une preuve afin de faire valoir un droit et le respect des libertés individuelles et collectives des autres. Le principe de proportionnalité est ainsi inscrit à l'article L.1121-1 du Code du travail en ces termes: « Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché ». Pour autant, il n'est pas toujours évident d'apprécier quand il y a atteinte aux libertés individuelles ou collectives : en témoigne toute la jurisprudence relative au courrier électronique, des dossiers et des fichiers informatiques des salariés.

B. La portée: l'exigence d'intégrité, d'imputabilité, de fiabilité

Transposer le raisonnement habituellement en vigueur à l'univers numérique n'est pas toujours simple. La loi du 13 mars 2000 érige l'écrit électronique au même rang que l'écrit papier mais conditionne néanmoins cette preuve à des exigences supplémentaires.

C'est ainsi que les juges ont eu à se prononcer sur la question de la copie numérique. En premier lieu, peut-on encore parler de copie lorsqu'il s'agit de document numérique dans la mesure où un document numérique se duplique à l'identique à l'infini? Les juges de la Cour de cassation semblent le penser. En effet, la deuxième chambre civile a rendu une décision le 4 décembre 2008 sur ce point sous le triple visa des articles 1334 et 1348 relatifs à la copie d'une part et d'autre part de l'article 1316-1 relatif à la preuve écrite. Le raisonnement consistant à faire une analogie entre la copie de document papier et la copie de document numérique peut s'expliquer par le souci de prendre en compte l'évolution des pratiques et l'embarras qu'elles occasionnent.

Par ailleurs, les juges vont être vigilants à apprécier exactement la portée des faits. Ils s'attacheront, par exemple, à distinguer la copie volontaire d'un fichier sur un ordinateur des copies automatiques. Selon l'hypothèse, la preuve ne sera pas la même. A titre d'illustration, on peut citer l'hypothèse où constitue deux infractions distinctes le fait de télécharger volontairement des images pédophiles d'une part, et d'autre part, le fait de les consulter sans les télécharger. C'est pourquoi, il sera demandé aux experts de vérifier si les copies des pages d'un site se trouvent ou non uniquement dans la mémoire temporaire de l'appareil.

Il en résulte, dès lors, que la technique probatoire doit sans cesse être adaptée en fonction de l'évolution du milieu numérique. Ces techniques qui seront amplement développées durant cette après-midi.

II.2. Critères d'appréciation technique, vraies et fausses preuves numériques

Monsieur Serge MIGAYRON : Expert de Justice près la Cour d'Appel de Paris

Pour être éligible au statut de preuve numérique, une information numérique doit satisfaire certains critères stricts avant de pouvoir faire l'objet d'une interprétation technique qui précèdera sa qualification juridique.

L'information numérique avant la preuve

Rappel des caractéristiques de l'information numérique

L'information numérique, ou *Electronically Stored Information* (« ESI »), est **facilement copiable** : L'Encyclopaedia Universalis, sans les images, peut ainsi être copiée en environ une minute par le port USB. Elle est **riche quantitativement** puisqu'on estime l'information numérique générée en un an par un individu dans le monde à l'équivalent de 800 romans et que 100 milliards de

courriels sont échangés quotidiennement dans le monde. Les systèmes numériques sont extrêmement prolixes en matière d'informations ce dont les experts profitent d'ailleurs lors de leurs investigations car ils trouvent souvent des informations créées à l'insu de l'utilisateur et dans des endroits discrets et parfois inattendus. Cette information est également **riche qualitativement**, plus que le papier. Par exemple, les propriétés (ou « métadonnées ») d'un document ou d'un fichier n'ont pas d'équivalents dans le monde de l'écrit non numérique. Cette information est **vulnérable**, de manière accidentelle ou intentionnelle. Elle peut **dépendre de son environnement**, matériel ou logiciel et, détachée de cet environnement, elle peut parfois être difficile à exploiter. Enfin, cette information est **effaçable** ... mais pas si aisément. Nous le verrons plus tard. Enfin, cette information n'est **pas toujours statique** et peut se présenter sous une forme dynamique la rendant plus difficile à capturer.

Qualité de l'information numérique

Les acteurs de la preuve numérique sont confrontés à des problématiques de choix de qualité de l'information que j'illustrerai avec l'exemple de la messagerie.

L'impression papier d'un courriel n'apporte généralement pas beaucoup d'informations sauf dans des cas très particuliers. Ainsi, un Expert a récemment sollicité mon avis sur un courriel imprimé qui était daté du mardi 21 Mai 2003 alors même que le 21 Mai 2003 était un mercredi ! Soit l'horloge de l'ordinateur ne fonctionnait pas (ce que je n'ai jamais constaté jusque là), soit ce courriel a fait l'objet d'une manipulation ... mais très grossière !

La **copie électronique d'un courriel** peut se faire, soit sans ou avec ses **données d'en-tête** (« header ») qui fournissent des informations très utiles sur l'adresse de l'expéditeur (équivalente de la boîte aux lettres où aurait été posté le courrier) de même que sur les centres de routage (équivalents aux centres de tris postaux) successifs qui l'ont acheminé.

Il peut également être procédé à la copie électronique complète du fichier de messagerie. Dans ce cas, il sera possible de rechercher des courriels effacés éventuels. Telle est la pratique de la DGCCRF qui procède par copies complètes des fichiers de messagerie lors de ses enquêtes. C'est une pratique que la DGCCRF justifie par des arguments sur l'intégrité et l'insécabilité qui sont très critiquables mais cette pratique bénéficie néanmoins, jusqu'à ce jour, d'une jurisprudence positive. Dans le cas d'une copie complète, le fichier de messagerie va toutefois être d'exploitation plus délicate puisque pourront être présents des courriers personnels ou des courriers d'avocats.

Enfin, la copie des fichiers de messagerie pourra être accompagnée de copies des fichiers de journalisation (fichiers « logs ») du serveur de messagerie, qui pourront apporter encore des informations complémentaires.

On voit donc, à travers l'exemple choisi de la messagerie, que les choix offerts sont multiples et permettent d'obtenir une information plus ou moins riche.

De l'information numérique à la preuve numérique : critères de qualification

Définition des critères

Le critère d'authenticité garantit l'origine de l'information. Le critère d'intégrité garantit le contenu de l'information. Le critère de traçabilité indique dans quelles conditions l'information a été copiée. Enfin, le critère de pérennité semble plus accessoire mais ne doit pas être négligé et est lié à la bonne conservation de l'information.

Confrontation de ces critères à la réalité

Parlons tout de suite de la signature électronique qui est un dispositif permettant de garantir l'authenticité et l'intégrité d'un document informatique, qui inverse même la charge de la preuve puisque l'article 1316 du Code civil stipule que « la fiabilité de ce procédé est présumée jusqu'à preuve contraire ». Ce dispositif répond donc aux deux premiers critères définis. Malheureusement, dans la pratique, l'information numérique signée électroniquement reste très minoritaire et il est donc le plus souvent nécessaire de s'en passer, pour évaluer les critères de qualification définis précédemment.

Critère d'authenticité

Le critère d'authenticité est un critère très exigeant qui est même sans droit à l'erreur (le sort d'individus peut en dépendre). Un compte de messagerie Lotus Notes, par exemple, est très sécurisé : La gestion des identités repose sur des moyens cryptographiques qui garantissent l'identité du possesseur du compte. Mais à l'inverse, les propriétés Windows d'un fichier

(« métadonnées ») sont très facilement modifiables, que ce soit de manière accidentelle ou intentionnelle. Ainsi, la simple consultation des propriétés d'un fichier modifie ces propriétés qui apparaissent donc très volatiles. Il conviendra alors de prendre de nombreuses précautions avant d'utiliser ces informations pour s'assurer qu'elles n'ont pas été altérées de façon volontaire ou accidentelle. Souvent, face à ce critère d'authenticité, l'expert aura intérêt à rechercher des faisceaux d'éléments d'identification convergents.

Critère d'intégrité

Le critère d'intégrité est également primordial.

Dans le cas d'une copie simple de fichier, il existe un outil nommé calcul d'empreinte numérique ou « hash » avec comme exemple l'algorithme MD5, qui permet d'attribuer à un fichier ou à un ensemble de fichiers une chaîne de caractères unique (on parle de fonction à sens unique ou irréversible). Quand le fichier est modifié, même très légèrement, son empreinte numérique change complètement. Ainsi dans le cas d'un fichier représentant un volume de l'Encyclopaedia Universalis (environ 7 millions de caractères), dans lequel une lettre seulement a été modifiée (le point final remplacé par un espace), les empreintes obtenues, totalement différentes, sont les suivantes :

Empreinte MD5 avant : A64C0C668E613B5D10B936F6BD2ED75D
Empreinte MD5 après : A616D59F9FC2E2671BB84F3621E41595

Un tel algorithme présente une hypersensibilité à tout changement, même infime. Aucune erreur n'est donc possible :

Deux fichiers, même différents de façon infime, ont des empreintes numériques totalement différentes.

Dans le cas de copie d'un support de données, comme un disque, différents modes de copie peuvent être utilisés : Une copie simple ou « logique » suffit si l'on ne recherche pas des fichiers effacés. A l'inverse, une copie physique (dite « bit à bit ») permettra de rechercher des traces éventuelles de fichiers effacés.

Parmi les **objets dynamiques** figurent par exemple les terminaux numériques mobiles et les disques SSD (« Solid State Drive ») qui utilisent des mémoires de technologie Flash. Les cellules de ces mémoires s'usent avec le temps et des microprogrammes sont chargés de surveiller leur niveau d'usure (« wear levelling »). A un certain moment, lorsqu'un niveau déterminé d'usure est atteint par une cellule, un mécanisme microprogrammé se met automatiquement en route et déplace l'information de la cellule usagée vers une nouvelle cellule. Un article très intéressant sur ce sujet, écrit par mes Confrères Jean-Louis COURTEAUD et Jean-François TYRODE, est paru dans le dernier numéro de la revue Experts. Ce mécanisme pourrait avoir pour conséquence que la signature MD5 du support concerné peut varier en fonction du moment où l'analyse est réalisée. Ce mécanisme est également mis en œuvre dans certaines clés USB de grande capacité, sans être documenté. Un tel mécanisme opère donc souvent à notre insu : Le simple examen de l'objet peut provoquer une modification de son contenu. Il convient donc que l'expert soit très vigilant.

Une solution consiste à effectuer une copie le plus tôt possible du support que l'on souhaite investiguer et de bien décrire les conditions dans lesquelles cette copie a été réalisée.

Dans les systèmes complexes, comme les plateformes électroniques d'enchères ou de vote, les calculs d'empreinte numérique sont très souvent inapplicables car ces systèmes sont dynamiques et leur état évolue pendant le vote ou l'enchère. Dans le cas d'une expérimentation, par exemple en tant que moyen de preuve pour des essais contradictoires en expertise, une double contrainte, de reproductibilité apparaît vis-à-vis d'une part de la situation historique du système (au moment où est apparu le litige) vis-à-vis d'une éventuelle contre expertise future d'autre part.

Critère de traçabilité

Le critère de traçabilité est le compagnon indispensable des critères d'authenticité et d'intégrité. On a vu avec les exemples précédents, qu'il est toujours nécessaire que les opérations réalisées soient précisément décrites. Il existe des moyens manuels de traçabilité mais également des moyens automatiques (en activant par exemple des fichiers de journalisation d'évènements ou « logs » sur un système).

L'exemple simple de gravure d'un CD rom permet d'illustrer l'importance du critère de traçabilité : Un CD rom est gravé successivement avec le graveur de Windows, avec un logiciel de gravure spécialisé (Easy Creator), sous la version 7 de Windows, sous la version Xp de Windows. Le fichier à copier a été créé le 1^{er} janvier. Sa gravure a été réalisée le 15 janvier. En fonction de chaque cas, les dates de création et de modification du fichier gravé (dates des onglets « General » et « Statistiques des propriétés du fichier ») sont les suivantes :

	Onglet général Créé le	Onglet général Modifié le	Onglet Statistiques Créé le	Onglet Statistiques Modifié le
Easy Creator Windows 7	1er Janvier	1er Janvier	1er Janvier	1er Janvier
Graveur Windows 7	1er Janvier	1er Janvier	1er Janvier	1er Janvier
Easy Creator Windows Xp	1er Janvier	1er Janvier	1er Janvier	1er Janvier
Graveur Windows Xp	15 Mars	1er Janvier	1er Janvier	1er Janvier

On constate que dans le cas d'usage du graveur de Windows sous Windows Xp, la date de la copie est prise comme date de création alors que dans les autres cas, la date de création d'origine du fichier est conservée. Donc, si l'on se retrouve avec un fichier gravé sur un Cd Rom et si on ne connaît pas le procédé utilisé pour la gravure, une erreur d'interprétation de sa date de création est possible. Il est donc bien indispensable d'accompagner toute opération de copie de fichier numérique d'une traçabilité rigoureuse.

Critère de conservation

Pour le critère de conservation, je citerai très rapidement le cas des CD et DVD en vous renvoyant à une étude réalisée par le Laboratoire National d'Essais (« LNE ») en 2004 qui montre que les durées de conservation effective de ces supports ne sont pas celles annoncées par les fabricants.

De l'information numérique à la preuve numérique : interprétation

Les conditions nécessaires à une interprétation fiable de l'information numérique sont donc bien l'authenticité, l'intégrité et la traçabilité sans oublier toutefois l'exploitabilité (puisque'il peut arriver par exemple que le format d'un fichier soit illisible ou que le fichier soit crypté).

Il est également nécessaire de tenir compte de limites possibles à l'interprétation puisqu'un résultat de recherche négatif, par exemple, pourra signifier soit que les fichiers recherchés n'ont jamais existé sur le disque, soit que ces fichiers ont existé puis ont été effacés, sans qu'il soit possible de trancher entre les 2 hypothèses.

Une autre limite à l'interprétation est liée, en France, au fait que nous Experts, ne pouvons pas avoir de certitude sur l'exhaustivité des informations qui nous sont communiquées par l'une ou l'autre partie. Le système américain avec la e-discovery est bien différent puisque'il a l'ambition, voire la prétention, d'appréhender la totalité de l'information numérique avant de commencer un procès.

Enfin, l'interprétation peut aussi varier dans le temps. En 2004, la presse a annoncé que l'algorithme MD5 aurait été cassé par une

équipe chinoise, ce qui n'était pas exact (cette équipe avait obtenu certaines collisions d'empreintes MD5, mais de façon fortuite, non généralisable : La fonction MD5 demeure irréversible). Néanmoins, si dans l'avenir l'algorithme MD5 était vraiment cassé, on entrerait alors dans une période d'incertitude pour les copies d'objets numériques, fichiers et disques, dont l'intégrité était sensée être garantie jusque là par des empreintes MD5.

Les conditions de validité de la preuve numérique

Pour être valable donc, une preuve numérique doit avoir passé avec succès une série de tests qui sont ceux de l'authenticité, de l'intégrité, de la traçabilité, de l'exploitabilité, de la pérennité et de l'interprétation.

Les acteurs de la preuve numérique doivent être rigoureux et très vigilants : L'erreur d'interprétation est possible car l'information numérique a tendance à se dérober à ces critères, en cas de défaut de méthode ou d'absence de précautions.

Finalement, ces critères de qualification ont un double but : D'une part permettre à la preuve numérique d'affirmer sa validité en résistant à la contestation, mais aussi permettre à une partie de disposer de moyens valables de la contester. Un parallèle peut être établi avec une théorie scientifique qui n'est vraiment scientifique que si elle dispose des qualités nécessaires à sa propre réfutation.

III. Constituer une preuve numérique

Participent à la table ronde :

*Maître Jérôme LEGRAIN, Huissier de Justice associé à Paris,
Christian AGHROUM, Chef de l'OCLCTIC,
Maître Olivier ITEANU, Avocat à la Cour,
David BILLARD, Expert de Justice près la Cour d'Appel de
Chambéry.*

*La table ronde est animée par Vincent VIGNEAU, Conseiller
référendaire à la Cour de Cassation, professeur associé à
l'université de Versailles Saint Quentin en Yvelines.*

III.1. Introduction

Monsieur Vincent VIGNEAU : Conseiller
référendaire à la Cour de Cassation, Professeur
associé à l'Université de Versailles Saint Quentin
en Yvelines – Membre du Laboratoire Dante

J'ai accepté avec grand plaisir de répondre à l'invitation de la CNEJITA et d'ouvrir cette discussion par quelques propos, ceux d'un juge, chez qui le sujet retenu, « *la constitution de la preuve numérique* » suscite le plus grand intérêt.

L'usage procédural de la preuve numérique est le fruit du long cheminement qui, depuis plusieurs années, a permis la reconnaissance de la valeur juridique des documents et de la signature électroniques. L'impulsion est venue de la Commission des Nations Unies pour le droit commercial international qui, pour la première fois, a adopté en 1996 une loi-type sur le commerce électronique.

Au niveau communautaire, une directive fixant un cadre juridique pour les signatures électroniques a été adoptée en 1999, suivie le 8 juin 2000 d'une directive sur le commerce électronique qui posait, pour la première fois, le principe de la reconnaissance de la signature électronique. Elle prévoit notamment que les Etats membres veillent à ce que l'efficacité juridique et la recevabilité comme preuve ne soient pas refusées à un acte au seul motif que la signature se présente sous forme électronique.

La transposition en droit français de cette directive fut réalisée par la loi du 13 mars 2000 qui reconnaît au vecteur électronique la même valeur juridique, la même validité et la même force probante que le document papier. Elle le fait en dépassant la conception implicite traditionnelle selon laquelle la notion d'écrit postule un support tangible en papier et en optant pour une approche fonctionnelle de l'écrit. Elle met fin ainsi à l'assimilation de l'écrit au papier : la preuve littérale est redéfinie en tant que telle afin de la rendre indépendante de son support. Elle ne s'identifie plus au papier et ne dépend ni de son support matériel, ni de ses modalités de transmission. La définition respecte ainsi le principe de neutralité technologique. La loi redéfinit la preuve littérale, ou la preuve par écrit, à l'article 1316 comme résultant « 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 leurs modalités de transmission ». Elle

admet même expressément l'écrit électronique à l'article 1316-1 qui dispose que « l'écrit électronique est admis en preuve au même titre que l'écrit sur support papier ». Mais l'écrit électronique ne suffit pas en soi. Pour disposer de la force probante, il doit s'accompagner de mesures accessoires qui garantissent l'existence de deux conditions qui sont considérées comme intrinsèques à l'écrit papier : l'auteur de l'écrit doit pouvoir être dûment identifié et l'écrit doit être établi et conservé dans des conditions de nature à en garantir l'intégrité. On notera cependant que même en l'absence de ces conditions, un écrit électronique peut constituer un élément de preuve. C'est ainsi que la Cour de cassation juge qu'un écrit électronique non sécurisé peut constituer une preuve dès lors qu'il est utilisé dans un domaine où la preuve est libre (en matière pénale ou de responsabilité délictuelle par exemple) et que la sincérité du détenteur n'est pas suspectée. Par conséquent, elle approuve une cour d'appel qui avait considéré qu'une saisie informatique d'une déclaration de créance auprès du représentant des créanciers pouvait faire pleine preuve de sa date. L'article 1316-2 vient enfin valider les conventions de preuve et laisse au juge le soin d'arbitrer entre les conflits de preuve littérale. Allant même au delà de ce que demandait la directive, la loi du 13 mars 2000 reconnaît, à l'article 1317, la valeur du titre authentique électronique.

On ne pouvait toutefois prétendre reconnaître l'écrit électronique sans reconnaître dans le même temps la signature électronique. Si, dans un écrit sous seing privé, la signature est un élément essentiel à sa validité, « l'exigence d'un manuscrit étant inconciliable avec l'échange de messages électroniques, force était d'admettre qu'il puisse exister un équivalent numérique à la signature traditionnelle » Pour ce faire, la loi du 13 mars 2000 reconnaît l'existence et la valeur de la signature électronique en adoptant une définition fonctionnelle de celle-ci qui se réfère aux

finalités qui lui sont assignées. Pour l'article 1316-4 du code civil, la signature doit remplir deux fonctions juridiques de base : l'identification de l'auteur et la manifestation de sa volonté, avec l'approbation du contenu de l'acte. Cet objectif est identique, que la signature soit manuscrite ou électronique. Mais on constate que, par rapport au support traditionnel, la loi en demande plus au support électronique qui, là encore, n'est pas en soi suffisant et doit être accompagné des mesures suffisantes pour en garantir d'une part le lien avec le document auquel il est attaché et, d'autre part, sa fiabilité. C'est l'objet du décret du 30 mars 2001 pris pour l'application de cet article qui a distingué, comme l'avait fait la directive, deux types de signatures électroniques : l'une, simplement indicative, se contentant de garantir son lien avec l'acte auquel elle s'attache, l'autre, sécurisée, ou renforcée, qui vaut jusqu'à preuve contraire.

La loi sur l'économie numérique du 21 juin 2004 achève la reconnaissance de l'écrit électronique. Elle accroît la portée de la loi du 13 mars 2000 relative à la signature électronique en étendant la reconnaissance de l'écrit électronique aux hypothèses où l'écrit n'a pas seulement pour fonction de constater l'existence d'un contrat, mais est exigé pour la validité même de l'acte. Ainsi, qu'il soit requis *ad probationem* ou *ad validitatem*, l'écrit électronique est soumis aux mêmes conditions que l'écrit papier.

L'ordonnance du 16 juin 2005 relative à l'accomplissement de certaines formalités contractuelles par voie électronique complète ce dispositif en généralisant l'écrit électronique. Elle insère ainsi dans le Code civil trois nouveaux articles (articles 1369-1 à 1369-3) qui autorisent, de façon générale, l'utilisation de la voie électronique dans le champ contractuel. Enfin, le décret du 28 décembre 2005 relatif à la procédure civile a autorisé l'usage de la communication électronique devant toutes les juridictions

civiles. Ainsi, désormais, les articles 748-1 et suivants du code de procédure civile font de la remise par voie électronique un mode ordinaire de remise des actes de procédure. Ces textes ne régissent cependant que la transmission des actes de procédure et non leur établissement qui est soumis au droit commun, doit être dressé selon les modalités prévues pour tous les actes électroniques.

Comme vous le savez sûrement, la Cour de cassation, juridiction plus que bicentenaire, a été la première juridiction suprême en Europe à dématérialiser sa procédure en matière civile. Cette dématérialisation, dont la généralisation a débuté l'année dernière, signifie que, désormais, les avocats aux Conseils ne sont plus tenus de produire à la Cour, à l'appui de leur pourvoi, un dossier constitué d'actes et de documents papiers. Ils peuvent, s'ils le souhaitent, adresser l'ensemble de leurs déclarations, mémoires, requêtes et productions de pièces sous une forme purement numérique et s'abstenir de les transmettre sur support papier. Ces actes et documents sont enregistrés sur le serveur de la Cour sous forme d'un dossier numérique, ensuite utilisé par les magistrats dont les travaux sont à leur tour intégrés sous un format numérique et diffusés immédiatement et directement à l'ensemble des acteurs du dossier. Dans un monde marqué par la place de l'écrit, le respect de délais et de formalités et le poids des traditions, l'idée de faire un jour disparaître le dossier papier au profit d'un dossier électronique, en conservant le même niveau de sécurité et d'échange, pouvait paraître une gageure. Mais la justice ne se réduit pas à la Cour de cassation. Bien au contraire, c'est d'abord dans les juridictions du fond que s'accomplit, grâce au travail et aux talents des magistrats et des auxiliaires de justice qui s'y dévouent, le miracle quotidien de devoir juger humainement des affaires humaines. La procédure ne se limite pas non plus à l'échange d'actes de procédure. Ceux-ci ne sont finalement que

les vecteurs des moyens échangés par les parties au succès de leurs prétentions et des éléments de preuve qu'ils soumettent à l'appréciation des juges. Or si, pour l'instant, le recours aux actes de procédure numérique est encore limité à la procédure devant la Cour de cassation, l'utilisation de moyens de preuve numérique par les parties elles-mêmes commence à se développer, au civil comme au pénal. Je tenterai de dresser une liste non exhaustive des différents modes de preuve numérique que l'on trouve dans le monde judiciaire : les méthodes d'investigation numérique destinées à la collecte, l'identification, la description d'informations numériques ; des informations présentées sous forme numérique, de façon brute, ou ordonnées en métadonnées ; des informations numériques contenant la preuve d'un acte ou d'un fait juridique ; des supports contenant des informations numériques avec l'exemple du SMS admis comme preuve numérique par la Première chambre civile de la Cour de cassation dans un arrêt du 17 juin 2009 ; des rapports décrivant les étapes d'une investigation numérique ou la saisie d'une information numérique, par exemple la saisie de données informatiques sur un ordinateur à l'occasion d'une visite domiciliaire sur le fondement de l'article L 450-2 du code de commerce selon l'arrêt du 17 juin 2009 de la chambre criminelle de la Cour de cassation ; des copies d'information numérique ; des empreintes numériques.

Cette table ronde nous offrira ainsi un panorama complet de la question. L'apparition de ces nouvelles formes de preuve ne manquera pas de nous conduire à rechercher dans quelle mesure elles remettent en cause la pertinence et l'efficacité de nombreuses règles et usages, à nous demander si leur coût et la facilité de leur mise en œuvre ne remet pas en question la position dominante dans laquelle se trouvait jusqu'à présent le ministère public dans la conduite des investigations et nous demander si la modernité des nouvelles technologies ne leur confère pas une

singularité telle qu'elle le ferait échapper par principe aux critères traditionnels de résolution des litiges.

III.2. L'huissier collecteur de preuve numérique volatile

Maître Jérôme LEGRAIN : Huissier de Justice associé à Paris

L'huissier de justice est désormais confronté aux preuves numériques. Professionnel de la preuve, il est coutumier de l'état des lieux locatif, du constat de dégradation... Dans ce monde réel, les règles sont connues et éprouvées. Avec les évolutions récentes, l'huissier de justice est désormais quotidiennement confronté au domaine virtuel. Dans ce monde, les règles de preuve restent à bâtir et l'huissier de justice doit continuer à collecter des preuves fiables et de qualité. Il est face aux difficultés de l'environnement technologique dont il n'est pas nécessairement familier. Comment assurer la qualité de la preuve et la justesse de son regard ? Comment garantir que les éléments relatés sont des certitudes ? Il est également confronté à l'environnement juridique dont les règles évoluent constamment ce qui ne lui facilite pas la tâche. Cette double difficulté dans l'établissement de la preuve numérique oblige l'huissier de justice à prendre les précautions maximales pour apporter une preuve de qualité, sachant que sa responsabilité est engagée et que les règles relatives à la preuve numérique sont en mouvement.

La difficulté de la preuve numérique dans l'environnement technologique

En l'absence de règles établies précisément, l'huissier de justice doit transposer les règles existantes. La preuve doit être loyale. Le constat d'huissier est exclusif de tout avis, il est la photographie d'une situation ce qui implique de respecter un certain nombre d'impératifs techniques pour garantir que la photographie est juste. Pour le Web 1.0, les règles sont désormais bien maîtrisées par les huissiers de justice et la jurisprudence est constante en la matière. Pour garantir la fiabilité des constats, les huissiers doivent prendre un certain nombre de précautions techniques qui consistent notamment de décrire parfaitement le matériel utilisé, de mentionner les adresses IP de connexion, de procéder à l'effacement des caches, des fichiers temporaires et des formulaires, de contrôler que la connexion se fait sans proxy... Dans le monde réel, l'huissier a l'habitude d'annexer une photographie : il transpose donc cette habitude dans le monde virtuel et peut annexer des impressions d'écrans ou de pages ou des captures d'images. Les huissiers de justice maîtrisent maintenant très bien ces procédures. Il est toutefois surprenant que les sanctions du non-respect de ces règles diffèrent puisqu'elles vont de la nullité du procès-verbal à l'irrecevabilité de la preuve ou au défaut de force probante. Le non-respect de ces règles techniques peut être admis pour d'autres organisations habilitées à dresser des procès-verbaux sur Internet, les tribunaux acceptant ces preuves, même imparfaites.

L'environnement technologique évolue plus rapidement que la jurisprudence et l'huissier se trouve face à des supports moins familiers et donc à de nouveaux challenges. Comment surmonter cette difficulté technique pour continuer à garantir la force de la preuve sans engager la responsabilité de l'huissier de justice ?

Pour ces nouveaux supports, l'huissier transpose donc les règles existantes. L'utilisation des nouveaux supports rend la frontière entre l'utilisation personnelle et professionnelle plus difficile à discerner. L'huissier peut collecter la preuve à partir de SMS, de terminaux mobiles, du Web 2.0, des vidéos, des réseaux sociaux, des forums et sites privés, des courriers électroniques, des espaces de collaboration de l'entreprise, des systèmes de visioconférence ou de géolocalisation. Pour tous ces outils, l'huissier de justice doit assurer la qualité technique de la preuve. Pour les SMS et les terminaux mobiles, l'huissier doit décrire très précisément le matériel présenté, les outils utilisés pour l'examen et les précautions techniques prises pour sauvegarder la preuve et la conserver. En ce qui concerne le Web 2.0, constitué de sites de partage et de réseaux sociaux, l'huissier doit garantir la loyauté de la preuve, sans masquer son identité, en transposant les règles relatives à l'accès au domicile et en s'imposant des contraintes techniques supplémentaires sur la loyauté de la preuve et le domicile, même s'il est virtuel. Pour le courrier électronique, il s'agit pour l'huissier d'aller le regarder en prenant un certain nombre de précautions, voire de le copier, de le sauvegarder et de le préserver pour une éventuelle expertise judiciaire ultérieure. La règle connue du secret de la correspondance est alors transposée. On aperçoit de nouveaux territoires dans l'établissement de la preuve, comme les espaces de collaboration des entreprises où l'information circule dans un espace partagé où le responsable devient seulement modérateur de données en mouvement. Comment tracer l'information et en rapporter la preuve.

La difficulté de la preuve numérique dans l'environnement juridique

En application du principe de précaution, les huissiers peuvent recourir au juge selon l'article 145 pour s'exonérer des

difficultés. Pourtant même dans ce cas de figure, des jurisprudences récentes nous emmènent vers une preuve difficile, voire impossible. Par exemple, la Cour de cassation a précisé, dans un arrêt du 9 avril 2009, qu'en matière de recherche de preuves, l'ordonnance requête doit être signifiée non seulement à la personne chez qui la saisie est réalisée mais également à la personne à l'encontre de laquelle un procès pourrait être engagé. Ce point est très difficile à maîtriser pour les huissiers de justice : s'il faut signifier une personne qui est à l'extérieur du lieu des opérations préalablement aux opérations de constat, cette personne peut alors détruire l'information avant même que l'huissier n'ait pu la sauvegarder. Des décisions récentes du Tribunal de Grande Instance de Paris annulent des procès-verbaux de constat d'achat faits sur Internet par des huissiers de justice et imposent d'utiliser la procédure de saisie contrefaçon. Je ne vois pas comment nous pourrions réaliser ce type d'opérations sachant qu'une ordonnance de saisie de contrefaçon doit être signifiée préalablement aux opérations de saisie. Les contraintes sont donc techniques mais aussi juridiques ce qui complique la tâche des huissiers de justice.

Monsieur Vincent VIGNEAU

Vous avez évoqué les problèmes de confrontation avec les nouvelles technologies et la procédure. J'ai noté notamment la question des règles applicables aux actes des huissiers de justice. Un débat a actuellement lieu à la Cour de cassation pour savoir si les actes des huissiers de justice de collecte de la preuve, comme les mesures d'expertise, sont des actes de procédures, régis par le régime de la nullité de l'acte de procédure. En fonction de la réponse donnée à cette question, la sanction diffère puisqu'elle peut être la nullité des actes de procédure, l'inopposabilité ou la privation du caractère probant. Ce point pourrait être tranché par

une formation solennelle de la Cour de cassation, tout comme la loyauté dans l'établissement de l'acte. A la rentrée d'octobre, l'assemblée plénière de la Cour de cassation tranchera cette question de l'usage de la loyauté et d'un mode de preuve obtenu de manière déloyale.

Après les avocats au Conseil et les notaires qui ont mis en œuvre la loi du 13 mars 2000 pour mettre en place des actes authentiques électroniques, quand les huissiers de justice dresseront-ils des actes authentiques électroniques ?

Maître Jérôme LEGRAIN

L'acte électronique d'huissier existe déjà. Les actes dits du Palais signifiés à la Cour de cassation se font par voie électronique. La signification de l'acte d'huissier aux sociétés et aux particuliers est en cours d'études avec la Chancellerie. La règle n'est pas encore totalement fixée et nous ne savons pas encore s'il faudra une acceptation préalable des signataires ou pas.

III.3. Police judiciaire et nouveaux territoires de l'information numérique

Monsieur Christian AGHROUM : Chef de l'OCLCTIC

Je suis chef de l'OCLCTIC - Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication - créé en 2000 qui succède à la BCRCI 1 créée en 1994. Ce service relève de la direction centrale de la police judiciaire. Comme tout office central, il a vocation à recueillir l'information et de la partager entre les différents services de police et de gendarmerie répartis sur l'ensemble du territoire national ; il est aussi le point d'entrée et de sortie unique dans notre domaine d'activité avec les autorités de police judiciaire étrangères. Nos offices centraux sont dotés d'équipes d'enquêteurs qui traitent des dossiers à vocation nationale et internationale.

Pour notre part, nous luttons contre la cybercriminalité, particulièrement celle à vocation économique. Nous sommes partis du piratage informatique pour nous ancrer de plus en plus dans le rôle d'une police du Web à travers une plateforme de signalement. Nos domaines privilégiés sont le « phishing » ou le « pharming », escroqueries commises par le biais de l'ordinateur. Nous avons également une fonction de support et d'assistance puisque nous formons l'ensemble des investigateurs en cybercriminalité ou policiers qui ont la charge sur l'ensemble du

¹ Brigade centrale de lutte contre la criminalité informatique

territoire national de procéder aux constatations ou aux enquêtes que nous menons au niveau national et international. Nous collaborons pour cela avec nos collègues de la gendarmerie nationale, très impliqués également dans la lutte contre la cybercriminalité à travers les effectifs dont elle dispose à Rosny sous Bois, à travers l'IRCGN² et le STRJD³. 450 personnes travaillent donc sur ce sujet, police et gendarmerie confondues, sur l'ensemble du territoire mais nous devrions bientôt être 600. Ce chiffre est faible par rapport à la réalité à laquelle nous sommes confrontés : la cybercriminalité évolue et se caractérise à la fois par la criminalité générée par les nouvelles technologies (informatique, internet, Web 2.0...) et par les escroqueries à distance ou commises sur Internet, apparues plus récemment que les autres en provenance d'Afrique, mais aussi par les infractions qui préexistent à ces nouvelles technologies mais sont grandement facilitées par elles : on parle ainsi de cyber-traffic de stupéfiants ou de cyber-pédopornographie, expression la plus connue de la manière dont une infraction peut se développer de manière incommensurable grâce à l'usage de ces technologies.

Nous disposons d'une plateforme de signalement – Pharos – qui a pour vocation de recueillir le signalement de l'ensemble des internautes, particuliers comme professionnels (fournisseurs d'accès et hébergeurs de sites).

Pour rechercher la preuve, l'enquête judiciaire est de plus en plus une enquête de confrontation des données et une enquête de traçabilité qui requiert d'aller chercher les preuves à l'étranger.

² Institut de recherche criminelle de la gendarmerie nationale

³ Service Technique de Recherches Judiciaires et de Documentation

Trois difficultés apparaissent alors. La première est liée à l'anonymisation puisque rien ne garantit sur Internet l'identité de celui qui est derrière le mail, la vidéo ou le site. La seconde difficulté concerne la traçabilité du fait de ces outils d'anonymisation mais aussi des outils de cryptologie qui permettent de chiffrer les données. Les chiffrements utilisés par la criminalité organisée ou par le terrorisme sont parfois très difficiles à casser, même si nous disposons en France d'un service doté des outils nécessaires. Les fonds engagés par l'Etat dans ce service ne suffisent pas toujours à obtenir des résultats probants du fait de l'extrême complexité de cette matière qu'est la cryptologie. Enfin, une troisième difficulté est liée à la conservation des données : une directive européenne impose une conservation des données en Europe de 6 à 24 mois. En France, les données sont conservées pendant un an. Or les données sont rarement aussi bien conservées à l'étranger. Dans une enquête classique, le temps de découvrir la victime et d'établir un lien entre la victime et l'auteur, ces éléments retardent l'accès aux données et compliquent l'avancée de l'enquête.

Nous avons établi des partenariats public/privé. L'enquête judiciaire est de plus en plus une enquête de traçabilité. Or les données sont détenues par tout le monde sauf par l'Etat puisque les fichiers de police ne contiennent pas beaucoup d'informations alors que, sur le Web 2.0 et les réseaux sociaux, on en trouve de nombreuses. Les banques, les fournisseurs d'accès ou les opérateurs de téléphonie mobile détiennent de nombreuses données et il faut donc obligatoirement nouer des partenariats public/privé. Nous sommes confrontés à des données de plus en plus lourdes et difficiles à exploiter. Il faudra se demander un jour s'il convient de les exploiter pendant le temps de la garde à vue ou en dehors de ce temps. Nous sommes inquiets quant à la possibilité de réaliser notre travail au mieux et au quotidien.

Vincent VIGNEAU

La frontière qui sépare en procédure pénale le PJ de l'expert s'estompe peu à peu devant le haut degré de technicité qu'ont dorénavant acquis vos collaborateurs. Un des problèmes auquel vous êtes confrontés consiste à concilier des règles fondées sur la territorialité de l'application des règles de droit et la dimension fondamentalement internationale de l'Internet qui se joue des frontières.

III.4. L'avocat ensemblier de preuves numériques

Maître Olivier ITEANU : Avocat à la Cour

Il est très important que des experts s'expriment sur ce sujet de la preuve numérique. Je crois que les juristes doivent bien savoir qu'il ne faut pas faire confiance à la preuve numérique et à la technique. Sur le plan de la sécurité, aucune technique n'est absolue, comme vous l'avez dit.

Je crois que la loi du 13 mars 2000 qui a modifié profondément notre droit de la preuve a mis en exergue un personnage central sur la question de la preuve : le juge. Certes, le juge ne peut pas rejeter une preuve au seul motif qu'elle est numérique, selon le principe de neutralité et de non-discrimination évoqué précédemment, mais le juge peut, s'il n'est pas convaincu, la rejeter à condition qu'il explique pourquoi cette preuve ne le convainc pas. C'est là que les experts ont un rôle à jouer. Ceci signifie que nous devons tous élever notre niveau de connaissances. A défaut d'être informaticien ou expert, nous

devons au fil des années devenir des connaisseurs en systèmes d'information. Cette question impacte donc le métier du juge.

Il m'a été demandé d'étudier l'impact de ces mêmes questions sur le métier d'avocat et j'ai choisi de vous parler, dans cette première table ronde sur la constitution de la preuve numérique, de la preuve et de l'identité numérique. Le relatif anonymat est une problématique qui se retrouve au final dans nos cabinets. Quand nous n'étions que dans le monde physique, le dossier était déposé et, s'il fallait parfois lever un K-bis ou poser quelques questions, l'identification du contradicteur ne posait pas de difficultés. Nous voyons maintenant arriver des dossiers où, pour tel contenu qui porte atteinte à un droit de tiers ou à l'ordre public, nous devons aider à l'identification de l'adversaire. Pour cela, les avocats se lancent donc dans une identification préalable de l'auteur de contenus, avec les outils dont ils disposent. Le fichier EDVIGE a levé beaucoup de boucliers. Il convient d'être vigilants par rapport à ces fichiers importants mais nous avons en réalité tous, experts ou pas, à disposition sur Internet un formidable outil de surveillance et des fichiers en très grande quantité. Si nous lançons une recherche avec le prénom et le nom sur un moteur de recherche comme Google, nous trouvons de multiples informations. Regardons les bases de données à notre disposition qui recensent les titulaires des noms de domaines, Infogreffe qui permet à tous de connaître les décisions judiciaires rendues dans la quasi-totalité des tribunaux de commerce, les bases INPI ou encore les réseaux sociaux (Facebook, Twitter, Viadeo, LinkedIn...)! Récemment, à l'occasion d'une plainte déposée auprès d'une autorité administrative indépendante qui a désormais des pouvoirs quasi juridictionnels, nous nous sommes rendu compte, simplement en regardant le profil LinkedIn de la personne désignée par l'autorité, que cette personne était une ancienne salariée de notre adversaire. Ces moyens sont à la

disposition de tous et impactent forcément le métier d'avocat. Enfin, il y a des traces, communément appelées « données techniques de connexion », que nous laissons à notre insu sur les sites Internet que nous visitons. Un site qui publie un texte, sous un pseudo, qui porte atteinte à un tiers. L'éditeur d'un site héberge ses contenus. Il faut alors identifier l'auteur de ce contenu avant d'envisager de le poursuivre et de constituer le dossier. Deux textes sont à notre disposition pour identifier l'auteur du contenu. Nous allons d'abord présenter une première requête auprès du juge des requêtes sur le fondement de l'article 6-II de la loi pour la confiance dans l'économie numérique du 21 juin 2004. Cette loi fait obligation à tout hébergeur fonctionnel de « conserver les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires ». Je suis l'hébergeur de mes enfants en tant que titulaire de mon compte d'accès Internet ; la BNP est l'hébergeur de ses salariés et a été condamnée dans un arrêt de la Cour d'appel de Paris rendu sur le fondement de la loi de 2000 pour n'avoir pas été capable de conserver ces données de nature à permettre l'identification. Le fait de ne pas conserver les données de nature à permettre cette identification est punie d'un an d'emprisonnement et de 75 000 euros d'amende. Si je présente une requête au juge des requêtes pour faire injonction à cette personne de nous communiquer les données techniques de connexion ou les données de nature à permettre cette identification de la personne ayant créé ce contenu portant atteinte au droit de tiers, l'éditeur de site aura au moins collecté les traces et l'adresse IP, suite de chiffres qui identifie le serveur utilisé par l'auteur du contenu illicite. Cette adresse IP appartient probablement à un des 15 fournisseurs d'accès qui regroupe 95 % de la population française. Avec cette information, je dispose d'un second texte, l'article L. 34-1 du Code des postes et des communications électroniques. Ce texte prévoit que, pour « des

besoins de la recherche, de la constatation et de la poursuite des infractions pénales et dans le seul but de permettre, en tant que de besoin, la mise à disposition de l'autorité judiciaire d'informations », les opérateurs de communication se voient imposer de conserver certaines catégories de données techniques. Au moyen de l'adresse IP, nous demanderons alors au juge des requêtes de faire injonction à tel opérateur de communication électronique propriétaire de cette adresse IP de dire à quel abonné il a distribué cette adresse IP à telle heure et dans tel fuseau horaire. Si l'abonné est un cybercafé en accès public, la situation est plus complexe mais nous pouvons, sur le fondement de l'article L. 34-1 du Code des postes et des communications électroniques, demander aux opérateurs de téléphonie mobile quels étaient les téléphones mobiles actifs sur cette zone de transit ou à cet endroit précis. Nous avons parfois l'impression d'être des gendarmes à la poursuite d'un voleur puisque nous remontons, avant même d'avoir constitué un dossier, jusqu'à l'auteur d'un contenu.

Le grand gagnant de la loi du 13 mars 2000, un peu critiquée en doctrine mais qui est pour moi une des meilleures lois des dix dernières années, est la vérité : malgré notre entrée dans l'ère numérique, nous n'avons pas perdu l'objectif de la vérité. Au final, cet objectif devra de tous : avocats, experts et juges.

Vincent VIGNEAU

Vous vous interrogez sur le point de savoir s'il fallait faire confiance à la preuve numérique mais je me demande s'il faut faire davantage confiance à la preuve traditionnelle. Je vous rappelle que nous avons récemment fêté le centenaire de l'affaire Dreyfus qui est partie d'un bordereau falsifié.

III.5. L'expert et les bonnes pratiques techniques

Monsieur David BILLARD : Expert de Justice près la Cour d'Appel de Chambéry

Le but d'une analyse d'un support numérique est d'obtenir une preuve, ou un élément de preuve, admissible devant une cour de justice. La difficulté de l'analyse est multiple ; elle est notamment liée au fait que le processus d'investigation modifie presque invariablement le contenu numérique du support et que l'analyse est liée à de nombreux aléas. La preuve sera donc parfois contestée et l'obtention de la preuve, ou le processus aboutissant à la constitution de la preuve, le sera bien plus souvent. En 2001, quand Zacarias Moussaoui était suspecté par le FBI d'être un présumé terroriste, ses ordinateurs portables avaient été saisis ainsi que les PC de l'université d'Oklahoma d'où il envoyait des e-mails. Le FBI avait alors copié les disques mais n'avait rien trouvé. Les avocats de la défense ont indiqué que le FBI n'avait pas acquis les disques de manière convenable et avait pu modifier les preuves : le FBI utilisait alors le CRC32 comme hash, plus faible que le MD5. Le FBI a donc dû refaire tout le processus d'investigation avec le MD5 pour prouver que les copies de disque avaient été bien réalisées.

Les bonnes pratiques ne sont pas nouvelles ; elles proviennent essentiellement des modèles scientifiques à l'œuvre dans les laboratoires d'expérimentation. McKemmish a théorisé les meilleures pratiques. Elles sont héritées de la compétence du personnel qui réalise l'investigation et sont liées à la

compréhension de la pratique par les autorités ayant ordonné l'expertise. En effet, plus les missions confiées à l'expert, sont précises, mieux il pourra répondre aux interrogations. Les bonnes pratiques évoluent constamment mais on peut dégager quelques fondamentaux.

Les étapes idéales sont les suivantes :

- l'ouverture et l'étude du dossier ;
- l'identification, la description et la sécurisation des données ;
- l'extraction des fichiers et des données ;
- l'analyse et le traitement des données ;
- la rédaction ;
- la restitution des scellés à la fin de l'investigation.

A l'issue de l'investigation, un rapport décrit précisément toutes les actions réalisées sur le support numérique et sur les données elles-mêmes. Il existe toutefois des contraintes de temps et de coût qui peuvent nuire à la qualité du dossier. Parmi les contraintes de temps figurent l'investigation en temps réel, les gardes à vue, les ordonnances sur requête : dans ce cas toutes les étapes idéales ne peuvent être respectées. Souvent la copie bit à bit des supports ne peut être réalisée car cela prend beaucoup de temps, sauf s'il s'agit du but de la mission. Les étapes d'identification peuvent être réalisées par une personne tierce afin que l'expert se concentre sur l'extraction des données et leur analyse. Des contraintes de coût s'ajoutent aux contraintes de temps : il peut s'agir de contraintes d'équipement et de compétence. S'il existe des logiciels libres, il faut parfois aussi acquérir des logiciels coûteux.

Les nouveaux supports comme les téléphones mobiles, les « skimmers » évolués, les GPS ou l'Internet sont devenus

intelligents. La mémoire flash modifie ainsi l'allocation des zones mémoires de son propre chef en fonction de l'usure. Pour se prémunir du mythe de la non-altération de la preuve numérique, il convient de journaliser toutes les opérations réalisées et d'indiquer les potentielles altérations. Des outils automatiques peuvent constituer une aide de ce point de vue.

Parmi les bonnes pratiques figure la gestion de la connaissance. Face à la complexité de l'investigation numérique, il convient de consulter et d'alimenter les forums et les blogs consacrés à l'informatique légale, d'échanger avec l'ensemble des acteurs (experts, magistrats, huissiers, avocats, forces de police et de gendarmerie), sans se contenter des forums francophones.

En résumé, les bonnes pratiques sont les suivantes :

- la connaissance du contexte (dossier pénal ou civil qui peut comporter les codes PIN) ;
- une démarche scientifique, rigoureuse et évolutive pour l'analyse en laboratoire ;
- une démarche pragmatique mais encadrée, pour l'analyse en temps réel ou à coût réduit ;
- la journalisation de toutes les actions faites sur le support ;
- l'indication des altérations possibles du contenu numérique (métadonnées, données).

Le praticien est donc condamné à se former et à contribuer à la formation. Ce point est absolument essentiel car il convient d'échanger sur les techniques.

III.6 Débat avec la salle

Un participant

Sur l'anonymat, vous n'avez pas parlé de l'usurpation d'identité.

Vincent VIGNEAU

Sur Internet, il est très facile de se constituer une sorte d'identité fictive, avec un alias. Cette question a repris une sorte d'acuité puisque les nouvelles règles qui régissent l'administration et les administrés font que les déclarations des administrés sont désormais créditées d'une présomption de fiabilité. Les originaux d'actes sont de moins en moins demandés et les copies sont acceptées. Des dispositifs purement déclaratifs auprès de serveurs Web permettent dorénavant d'accéder à des formulaires de Sécurité sociale ou à des souscriptions de contrat. Se posent alors des questions d'escroquerie et de faux, du fait de toutes ces méthodes d'usurpation d'identité amplifiées par le recours aux nouvelles technologies.

Christian AGHROUM

Quand nous parlons d'anonymisation, nous incluons cette notion d'usurpation d'identité. Il est ainsi possible de créer une identité totalement fictive ou d'en utiliser une. Nous retrouvons de telles pratiques dans la pédopornographie où les adultes se font passer pour des enfants mais aussi dans la plupart des affaires d'escroquerie auxquelles nous sommes confrontés sur Internet comme dans le monde réel.

La difficulté actuelle consiste à établir l'infraction : c'est pourquoi la LOPPSI – loi orientation et de programmation pour la performance de la sécurité intérieure – définit cette infraction d'usurpation d'identité numérique qui n'existait pas jusqu'à présent ce qui est fort utile car la plupart des infractions commises sur Internet le sont désormais avec utilisation de cette identité falsifiée.

Un participant

Vous parlez tout à l'heure de constat sur Internet en évoquant la notion de domicile. Quelle est alors la limite entre constat libre et constat sur requête du juge ?

Maître Jérôme LEGRAIN

La limite n'est pas toujours facile à fixer : je la fixe lorsqu'on doit me consentir un accès en sachant qui je suis. Si je peux accéder au site en ayant fait connaître mon identité, à partir du moment où je reçois les identifiants et le mot de passe, je peux aller sur ce site. A partir du moment où j'accède à un site sans communiquer mon identité, avec un simple pseudo, et que je reçois un code d'accès, je franchis en revanche la limite. Le problème se pose quand on requiert une ordonnance au titre de l'article 145 à qui doit-on alors la signifier ?

Maître Olivier ITEANU

La loi Godfrain de 1985 crée le délit de fraude informatique et le délit d'accès ou de maintien frauduleux à un système de traitement des données. Nous sommes parfois dans un domicile privé virtuel.

Un participant

Dans un cas concret, un huissier a obtenu des informations de la part d'un site Internet et communiquant son nom de jeune fille pour ne pas éveiller les soupçons.

Maître Jérôme LEGRAIN

La question de la loyauté de la preuve se pose alors.

Vincent VIGNEAU

La jurisprudence est claire sur ce point et sanctionne l'huissier de justice qui procède à un constat ou à une interpellation en masquant sa véritable qualité. La preuve est alors déloyale et ne peut servir de fondement à une décision.

Maître Olivier ITEANU

Dans l'affaire Kitettoa, la Cour d'appel de Paris a jugé une personne entrée par erreur, à la suite d'une faille de sécurité, sur un site Internet. Lorsqu'on est dans un lieu où on ne devrait pas être, la preuve est déloyale, même si le code d'accès n'est pas requis. .

Yves LEON, Expert de justice près la Cour d'Appel d'Aix-en-Provence

La signature numérique doit-elle être accompagnée d'un certificat ?

Michel ENTAT, Expert de justice près la Cour d'Appel de Paris

Oui. La signature numérique est présumée fiable ; elle doit être réalisée avec un dispositif de signature sécurisé et un certificat qualifié. Il n'existe presque pas de certificats qualifiés, du moins référencés par le Ministère de l'Economie et des Finances. En tant que technicien, je suis persuadé de la fiabilité de la signature électronique. Si le dispositif est fiable, réalisé avec un dispositif de signature adéquat et un certificat électronique remis en face à face, l'intégrité des fichiers et l'authentification du signataire sont alors sûrs mais il existe pourtant un vide énorme sur la portée de la signature puisque le même dispositif technique est utilisé pour signer un acte d'engagement dans les marchés publics et pour signer une facture à seule fin d'en garantir l'intégrité dans le cas d'un éventuel contrôle fiscal. Comment est-il envisagé d'attester de la portée d'une signature électronique ?

Vincent VIGNEAU

Sur le plan juridique, la signature manuelle présente la même fiabilité. La jurisprudence admet aussi des signatures par apposition de griffes. Nous sommes donc dans la même configuration.

Michel ENTAT

Quand on appose une signature électronique, on peut intégrer à ce fichier de signature des paramètres complémentaires qui stipulent par exemple que la signature ne vaut que pour une partie du fichier joint ou que pour garantir l'intégrité. En tant qu'expert de justice, je peux signer un fichier dont j'ai participé à la saisie pour être sûr qu'il ne soit pas modifié ou pour indiquer que

j'ai réalisé la copie, ce qui ne signifie pas du tout que j'approuve son contenu.

Isabelle RENARD, avocat

Cette question se pose dans de multiples contextes, pour les factures ou l'environnement réglementaire pharmaceutique. Dans ce dernier exemple, les acteurs de la chaîne signent les fichiers numériques et se demandent si cette signature impose le consentement au fichier. Or la portée de la griffe manuscrite n'équivalait pas à un consentement. Nous avons toujours eu un problème relatif à la portée de l'écrit ou de la signature et cette question n'est pas nouvelle.

Yves LEON

La question ne se pose pas avec une signature complètement constituée, certificat à l'appui. A partir de quel moment cette signature numérique peut-elle être considérée comme suffisante ? Lorsque je communique le numéro de ma carte bancaire pour payer un achat en ligne ainsi que mon identité, est-ce une signature numérique ?

Vincent VIGNEAU

Ce n'est alors pas une signature électronique mais ce pourrait peut-être être considéré comme un commencement de preuve par écrit. Nous devons alors appliquer les règles de droit commun. La signature électronique résulte d'un processus signé par décret avec l'intervention d'un tiers certificateur. Toute empreinte de consentement doit être appréciée comme telle. L'apparition de votre numéro facial de carte bancaire n'est pas de nature en soi à prouver votre consentement mais si, en plus, vous

ne déposez pas plainte et que le bien commandé est bien livré à votre domicile, il est probable que le juge considérera que ces éléments établissent de manière suffisamment certaine la preuve de votre consentement. Nous sommes alors dans les présomptions de l'homme qui consistent à déterminer comment le juge tire un fait inconnu à partir des faits connus. La dématérialisation ne présente pas une singularité telle qu'on appliquerait d'autres règles que les règles générales du Code civil.

IV. Exploiter une preuve numérique

Participent à la table ronde :

David BENICHOU, Vice Président chargé de l'Instruction au Tribunal de Grande Instance de Nanterre,

Jean-Pierre LUCQUIN, Juge consulaire, Délégué Général au Tribunal de Commerce de Paris,

Maître François-Pierre LANI, Avocat à la Cour,

David ZNATY, Président de la Compagnie des Experts agréés par la Cour de Cassation, Président de la CEESD.

La table ronde est animée par Monsieur Nathan HATTAB, Président de la CNEJITA.

IV.1. Introduction

Nathan HATTAB : Président de la CNEJITA

Le thème de notre table ronde porte sur l'exploitation de la preuve numérique collectée. Avocats, juges, huissiers de justice et experts, nous sommes tous amenés à travailler sur cette matière numérique et tous de façon complémentaire.

Nous sommes confrontés à une apparente simplicité de cette information numérique, qui peut nous induire à des erreurs d'appréciation si nous ne procédons pas méthodiquement.

Confronté aux difficultés de l'objet numérique et à la complexité des situations, les experts sont dans l'obligation de se poser de nombreuses questions qui les forcent à l'application des bonnes pratiques, à la vérification et au recoupement.

Quelles sont les attentes du juge pénal en la matière ?

IV.2. Le Juge pénal, ses attentes, une preuve sûre et intelligible

Monsieur David BENICHOU : Vice Président en charge de l'Instruction au Tribunal de Grande Instance de Nanterre

Avant d'entrer dans le vif du sujet, je souhaiterais, à titre de transition, inviter ceux qui souhaitent réfléchir au concept de signature électronique, à lire l'excellent ouvrage de Béatrice Fraenkel, professeur de linguistique à l'Université René Descartes, « La signature, genèse d'un signe », publié aux éditions Gallimard. Pour moi, mais ça n'est pas l'objet de mon exposé, le concept même de signature électronique, relève d'un tour de passe-passe, qui fait croire à l'homme que l'on parle de la signature qu'il connaît habituellement, celle qu'il peut faire avec un simple stylo. Or tout cela mériterait de longs débats, qu'un autre colloque, nous permettra je l'espère de poursuivre.

Venons-en à mon propos sur les attentes du juge pénal à l'égard de l'expert en informatique.

En procédure pénale, le principe de la liberté de la preuve, hors matières spéciales (ex: agents spécialement assermentés en matière de contrefaçon), fait que l'on devrait davantage parler d'éléments de preuve numériques, plutôt que de "preuves numériques" ; celles-ci étant plus une facilité de langage qu'une notion juridique aux contours précis.

Pour nous la preuve numérique ou électronique, s'entend de toute information contenue dans un objet que l'homme n'est pas en mesure d'examiner par l'usage de direct ses sens (ex: contenu d'une clé USB, code source d'un site web, contenu d'un disque dur ou d'une carte à puce...). La « preuve numérique » couvre également ce qu'une personne normalement sensée ne peut interpréter en raison de son caractère technique (ex: une ligne de code en langage informatique).

Pour apprécier la valeur probante de ces éléments, comme des rapports des experts, la procédure pénale laisse au juge toute liberté d'appréciation, l'intime conviction restant le principe, sous le feu de la discussion des parties, expression principe du contradictoire.

En ce sens le contradictoire, plus que toute préconisation technologique, toujours précaire, est la meilleure des garanties d'une bonne utilisation judiciaire des preuves numériques.

1. Attente au regard des missions des experts

1.1. Les mission pour rendre sensible l'insaisissable, ou missions « pour voir »

Ce sont toutes les missions qui servent à transférer dans une forme interprétable par l'homme le contenu des objets

techniques (on pourrait même dire "transmuter" tant le saut qualitatif est grand entre microprocesseur et un document imprimé sur une feuille de papier ou affiché en langage humain).

Exemple : imprimer les images contenues dans un disque, les correspondances d'un compte email, etc.

On pourrait presque les appeler de missions "pour voir" car tout ce qui échappe aux sens des parties et du juge restera occulté du débat (une image n'existe que parce qu'on peut la voir et qu'on est capable d'en apprécier le contenu, la discuter, c'est évident pour un document écrit).

Ces missions sont peu techniques (hormis les problématiques de recouvrement de données ou de données masquées, cryptées), en ce sens qu'elles ne réclament pas toujours un haut niveau de compétence grâce à des outils automatiques comme "Encase".

En revanche les précautions et une rigueur dans la méthodologie doivent être observées par l'expert (point 2), car les "métadonnées" du document peuvent aussi donner lieu à débat (date, accès, propriétés, etc.).

1.2. Les missions comportant une réelle question technique

Soit l'affaire a mis en évidence un problème technique clairement identifié, (exemple : les caractéristiques de la machine de untel sont-elles compatibles avec les traces d'intrusion repérées sur tel système), soit une mission "pour voir" soulèvera des problématiques spécifiques comme :

- l'usage de procédés tendant à cacher ou brouiller l'information (cryptographie, stéganographie);

- la question délicate de la datation des opérations réalisées sur les fichiers et leur imputation à un agent agissant sur le système;

Des questions rédigées dans la mission pourront porter précisément sur ces points:

- A-t-il été fait usage d'un procédé de chiffrement ? le cas échéant le décrire, etc.

2. Attente au regard de l'ensemble du processus de recueil et d'expertise

2.1. La traçabilité

Il s'agit de pouvoir connaître précisément l'origine du moyen de preuve, et les différentes opérations qui ont pu être réalisées jusqu'à ce que le moyen de preuve ait pu être gelé ou préservé dans un état stable.

Exemple : saisie du poste de travail d'un salarié, quid de ce qui s'est passé sur ce poste entre le départ du salarié et l'éventuel placement sous scellé ?

Il s'agit également de la traçabilité du travail de l'expert: matériels utilisés, logiciels, méthodologie précise. Cette traçabilité est précieuse car:

- elle montre que l'expert n'a rien à cacher sur sa manière de travailler (crédibilité) ;

- elle permet aux parties de discuter certains points.

La transparence sur les méthodes de travail, loin d'affaiblir le travail de l'expert le consolide et donne au contradictoire son terrain commun.

2.2. La préservation de l'intégrité de l'élément

C'est bien sûr la possibilité de faire procéder à une contre-expertise ou à des compléments d'expertises. La fabrication de copies de travail laissant inaltéré le support original est une bonne pratique. Si l'on peut garantir que l'humain n'altère par la preuve numérique, grâce à l'apposition de scellés, le support lui-même se dégrade au cours du temps. Ceci pose naturellement des problèmes

Exemple : impossibilité de visionner des enregistrements de vidéo surveillance plusieurs années après les faits, non pas à cause des logiciels, mais à cause de l'altération des supports physiques de type DVD

2.3. La prise en compte du contexte dans l'extraction d'éléments

Toute expertise "pour voir" doit remettre les éléments dans leur contexte. C'est le principe de la juste appréciation du contenu d'une bibliothèque: en se concentrant sur un rayonnage seulement on peut lui donner un caractère qu'elle n'a pas.

Exemples :

-10 sites pédopornographiques parmi 1000 sites ne signifient pas la même chose que 10 parmi 100

- Une bibliothèque qui contient beaucoup de livres, tant sur les armes que sur les objets en général, en ne parlant que de ceux

sur les armes, on lui donnera un caractère orienté qu'elle n'a pas en réalité.

2.4. La rigueur dans les termes utilisés par l'expert

C'est une évidence, mais l'expert ne doit se prononcer que pour des questions entrant dans son office.

- Exemple : imprimer des fichiers pornographiques: oui mais dire que certains sont pédopornographiques et d'autre pas, non, c'est du domaine de juge, pas de l'expert, qui est expert en informatique pas en interprétation des images à caractère sexuel; dans ce cas on usera de précaution sémantiques: fichiers pouvant représenter des mineurs (hors les cas où la minorité apparaît comme manifeste, idem pour le caractère sexuel des images);

- Exemple : à proscrire absolument: untel s'est rendu coupable de contrefaçon ou d'intrusion...pour telle ou telle raison, l'expert n'est ni enquêteur, ni juge

Nathan HATTAB

En premier lieu et au-delà des doutes sur la signature électronique, les avocats et les magistrats seront soumis à la numérisation des échanges des actes de procédures dans peu de temps. Les greffes des juridictions, comme les cabinets d'avocats s'organisent pour faire face à cette numérisation des échanges. Cette réalité du numérique est toute proche, avec ses contraintes en matière d'authentification et de préservation de l'intégrité des données échangées.

Quant aux attentes du juge pénal et au comportement de l'expert de justice, je voudrai souligner que l'expert de justice ne travaille ni à charge ni à décharge et qu'il ne doit pas exprimer d'opinion subjective.

Dans les expertises judiciaires, il nous est demandé de répondre à des questions précises, mais souvent aussi à une question ouverte. En expertise pénale, nous avons une phrase qui apparaît dans les missions de façon récurrente «Faire toute observation utile à la manifestation de la vérité. », pour éclairer le juge si nous constatons un élément important lors de nos investigations.

Il en est de même en expertise civile avec le point de mission « *Fournir tous éléments procédant de son domaine de compétence, afin d'éclairer la juridiction éventuellement saisie sur les origines et les causes techniques des faits litigieux allégués ...* ».

IV.3. Exemples de difficultés rencontrées par le Juge chargé du Contrôle des Expertises

Jean-Pierre LUCQUIN : Juge consulaire,
Délégué Général au Tribunal de Commerce de
Paris

La preuve en matière civil doit respecter les principes généraux énoncés par l'article 1315 du Code civil qui édicte deux règles dont l'une concerne directement le sujet : « *celui qui réclame l'exécution d'une obligation doit la prouver* ». Il en résulte que le juge ne peut pas tenir un fait avéré en se fondant sur de

simples allégations de la partie sur laquelle repose la charge de la preuve. Par ailleurs, la preuve des actes juridiques civils ne peut être apportée que par des moyens de preuve de caractère parfait, sauf dérogation légale. La preuve des faits juridiques est libre, selon les dispositions de l'article 1348 du Code civil, sauf interdiction légale, étant rappelé que les actes de commerce peuvent se prouver par tous moyens, à moins que la loi n'en dispose autrement. L'article 1316 du Code civil assure à l'écrit sur support électronique la même force probante que l'écrit sur support papier.

Or, comment convaincre un tribunal de commerce du bien fondé des prétentions quand la preuve est apportée par des éléments se trouvant sur le disque dur d'un ordinateur, dans une boîte aux lettres électronique ou dans un réseau ? La preuve devra emporter la conviction du juge qui ne pourra la rejeter qu'à une double condition : si elle ne le convainc pas, il devra expliquer pourquoi et son rejet devra être motivé.

La clarté des dispositions en cause régissant la preuve numérique paraît faciliter une application aisée. Reste que la réalité s'avère beaucoup plus complexe et aléatoire compte tenu du caractère modifiable et falsifiable des données. Ces dispositions sont appliquées par un juge qui n'est généralement pas familier des techniques susceptibles d'effectuer la démonstration de la preuve de manière parfaite. Plus que dans d'autres domaines, le juge est confronté à une difficulté de compréhension et d'appréciation de la crédibilité et de la fiabilité des éléments la preuve. Il aura donc tendance à recourir à une mesure d'instruction, comme au pénal, dont la définition de la méthodologie et la réalisation s'avèrent aussi assez complexes.

Le juge aura à apprécier le degré de résistance de la preuve à la contestation et sa capacité à être contestée, étant entendu qu'une preuve qui ne serait pas contestée sera exposée au doute. Jusqu'à présent, il n'existe pas de jurisprudence de référence émanant de la Cour de cassation en matière commerciale. Pour le tribunal de commerce de Paris, nous avons retenus deux cas récents qui présentent un intérêt. Dans le premier, dans le cadre d'une saisie de contrefaçons, le tribunal avait ordonné la communication d'un logiciel à la date de la saisie qui avait été refusée par la défenderesse à l'huissier instrumentaire à une date antérieure. Lors des opérations d'expertise, la défenderesse a déclaré ne disposer d'une version de la pièce postérieure à la date de saisie. Cette situation ne permettait pas d'écarter la possibilité d'une modification ultérieure entre la date de saisie et celle de la communication. Le juge du contrôle a décidé de poursuivre l'expertise afin de mettre en lumière des analogies structurelles entre les logiciels en cause qu'aucune modification ne peut faire disparaître ou bien l'existence de différences structurelles trop importantes. Le second cas concerne un employé qui a rendu, lors de son départ, le microordinateur qui lui avait été confié. Quelques semaines après, l'employeur examine le contenu du disque dur et déclare à l'expert avoir constaté la présence, dans ce microordinateur de fichiers de nature confidentielle. L'employeur sauvegarde les fichiers, formate le disque dur et confie l'ordinateur à un nouvel employé. Il fait ensuite appel à un sachant technique pour établir le constat. Le sachant examine le contenu du microordinateur et constate la présence des fichiers confidentiels ainsi qu'une modification de la date du système du microordinateur. L'affaire sera prochainement en délibéré.

Nathan HATTAB

Dans ces deux cas présentés, l'intégrité de l'information pourrait effectivement être remise en cause.

Dans le cadre d'une expertise pénale, il m'est aussi arrivé d'examiner un ordinateur avec des scellés qui n'empêchaient aucunement d'accéder au disque dur, et donc aux informations enregistrées. J'ai fait part de mon constat au juge d'instruction qui m'a demandé de continuer l'expertise du disque dur. J'ai bien entendu, signalé, dans mon rapport l'état des scellés et les risques relatifs à l'intégrité des données analysées.

Dans le cas de l'expertise civile, présenté par Monsieur le Président LUCQUIN, l'examen des logiciels peut effectivement aboutir à l'identification d'éléments technique à charge ou à décharge.

David BENICHO

Lors d'un récent conflit au pénal entre un employeur et un salarié pour fraude informatique, l'employeur a confié l'ordinateur à un huissier. Le juge a confié ensuite la machine à un expert. La traçabilité du scellé permettra ensuite de comprendre ce qui s'est réellement passé. Si le scellé a eu une vie avant d'arriver chez l'huissier, l'expertise montrera ce que l'ordinateur a vécu avant d'avoir été placé sous scellés.

IV.4. La dissymétrie de la charge de la preuve et coût

Maître François-Pierre LANI : Avocat à la Cour

Le métier d'avocat a changé et l'avocat doit désormais être un ensemblier d'éléments de preuve, notamment sur les problématiques numériques. Ceci est cependant réservé à une partie assez réduite de la profession. Le contentieux lié à la preuve numérique est un exercice extrêmement difficile pour l'avocat car il existe une certaine complexité à établir la preuve électronique : même si elle laisse des traces, elle n'en demeure pas moins de plus en plus complexe et, surtout, elle ne permet pas, la plupart du temps, de vérifier les critères d'authenticité, d'intégrité et de traçabilité.

Si la preuve est facile à "récupérer", la preuve numérique doit être recueillie dans des conditions incontestables, c'est-à-dire généralement contradictoires et conservée dans des conditions telles qu'elle ne puisse être altérée, pour ne pas être contestée ultérieurement par celui auquel on l'oppose.

Ainsi deux idées s'opposent :

D'un côté, la preuve numérique semble très accessible car les nouvelles technologies laissent énormément de traces et offrent un champ très large de possibilités pour la constitution de la preuve, et ce, dans une apparente facilité ;

D'un autre côté, la preuve numérique n'est pas facilement exploitable devant un tribunal compte tenu de l'exigence de plus en plus forte des juges quant aux règles d'établissement de la

preuve (dès lors que ces preuves peuvent être manipulées facilement sans qu'il soit besoin d'être ingénieur informatique).

Le praticien rencontre encore des difficultés à obtenir des éléments d'information, notamment la communication de l'adresse IP par le fournisseur d'accès à Internet. Le praticien est encore confronté à d'autres exigences : le respect de la vie privée, de certains éléments de confidentialité et du secret des affaires.

Deux cas concrets soumis dernièrement à mon cabinet permettent de bien illustrer le propos.

La preuve informatique dans l'expertise judiciaire

La tendance de ces dernières années a été de se priver de l'expertise informatique et donc de la preuve numérique ; d'aucuns considérant que les éléments du dossier et les éléments de fait étaient suffisants pour voir reconnaître leurs droits.

Les parties ont fait ainsi l'économie de la preuve technique / numérique. L'argument principal était que l'expertise judiciaire est fort onéreuse et longue.

Cependant, l'absence d'expertise judiciaire permettant de certifier que les éléments de preuve apportés par le demandeur étaient incontestables a conduit à des procès qui sont terminés dans la majorité des cas par un débouté des demandes pour défaut d'établissements des griefs allégués.

La constitution de la preuve dans le cadre d'une expertise judiciaire est longue et suit un processus devant être respecté :

- rétablir l'environnement querellé en demandant notamment à la partie à l'initiative de l'expertise de :

- démontrer que la sauvegarde effectuée non contradictoirement reflète le complet périmètre fonctionnel et technique du logiciel ;
- apporter les garanties suffisantes que tous les programmes de la solution ont bien été sauvegardés au jour de la constatation des dysfonctionnements allégués.

A défaut, il y a un risque que la partie adverse considère que les tests qui sont effectués dans le cadre de l'expertise ne respectent pas le principe du contradictoire et ne bénéficient pas de la garantie d'exhaustivité permettant de considérer que ces tests ont été faits dans une situation technique et fonctionnelle identique à celle qui existait à la date à laquelle les dysfonctionnements reprochés ont été découverts.

- exposer les griefs ;
- procéder aux tests sur la base de ces griefs ;
- nourrir le contradictoire.

Toutefois, même dans les cas où un tel processus a été suivi sur une version validée par l'expert avec des dysfonctionnements constatés (certes relativisés voire contestés parce que jamais allégués), il est arrivé que l'expertise échoue.

Exemple : Le premier cas concerne des dysfonctionnements dans un système progiciel. Bien que la

sauvegarde n'ait pas été effectuée contradictoirement par le requérant à l'expertise judiciaire au visa de l'article 145 du Code de procédure civile, les parties ont considéré toutefois que cette sauvegarde était la bonne et ont collaboré en toute bonne foi. Des tests ont ainsi été effectués sur cette version validée par l'expert. La procédure d'expertise s'est déroulée, avec sa longueur, sa complexité. Des dysfonctionnements ont été constatés. A la fin de l'expertise, il a été constaté sur la base d'un simple e-mail qu'à un moment donné, un correctif mis à la disposition du client n'a pas été installé par ce dernier alors qu'il en avait la charge (il était en autonomie sur la mise en place des versions du logiciel). Cet e-mail a fait tomber l'expertise car il est alors devenu impossible pour l'expert de garantir que les dysfonctionnements constatés ne résultaient pas de l'absence de mise en place de ce correctif. Toute l'expertise judiciaire a alors été intégralement remise en cause. Le doute a ainsi été créé et l'expert ne pouvait garantir l'authenticité, l'intégrité et la complétude de la preuve électronique dès lors qu'un correctif a été livré. La position est claire : il s'agit de créer le doute dans l'esprit du magistrat car l'expert ne pourra pas garantir que la solution sauvegardée aurait été la même si le correctif avait été téléchargé par l'utilisateur.

Cet exemple démontre que la preuve informatique est toujours difficile à apporter même dans un processus rigoureux suivi par l'Expert et les parties au litige.

La preuve informatique dans le contentieux social

Là encore, j'illustrerai mes propos d'un cas réel suivi par mon cabinet.

Exemple : La Direction juridique et la Direction des systèmes d'information d'un grand groupe ont saisi le cabinet. La DSI d'une entreprise a constaté, de manière fortuite, que les e-mails des messages électroniques professionnels de certains de ses salariés ont été, à l'insu de l'entreprise et de ces salariés, copiés et détournés (par le biais d'une copie cachée) vers une adresse internet inconnue (mais comportant la même extension que les autres adresses e-mails de l'entreprise)

Le responsable de la sécurité informatique a en effet mis en place, au niveau du serveur informatique, un système de détournement des mails de la direction générale vers son PC personnel à son domicile. Ces messages ont été consultés à distance via une connexion internet dont l'adresse IP a été identifiée.

=> Un constat d'huissier a été effectué pour constater techniquement l'existence de ce détournement. Le constat a confirmé le détournement et a fait notamment état de l'identité du fournisseur d'accès internet ayant attribué cette adresse IP.

Par requête 145, il a été demandé (de manière non contradictoire) au juge d'autoriser un huissier à se rendre dans les locaux du FAI afin de se faire remettre les éléments d'information permettant l'identification du titulaire de l'adresse IP.

Le FAI a refusé de communiquer les informations sur le fondement de l'article L. 34-1 du Code des postes et communications électroniques car selon lui ces éléments d'informations ne peuvent être communiqués que sur réquisition pénale.

L'article L.34-1 du Code des postes et des communications électroniques a un champ d'intervention très limité puisqu'il stipule que « pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales et pour la prévention du téléchargement illégal », les fournisseurs d'accès doivent permettre, pendant un an, de recueillir les données exclusivement mises à la disposition de l'autorité judiciaire. Le dispositif de l'article 6 de la loi du 21 juin 2004, dite loi LCEN, fait obligation aux fournisseurs d'accès et aux hébergeurs de conserver les données « de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires ». Ces dispositifs légaux ont ainsi des périmètres réduits. Dans l'affaire précitée, l'auteur a néanmoins reconnu les faits dans la mesure où une action au fond avait été lancée. Il faut noter que les adresses IP octroyées en mode Free wifi ne permettent pas techniquement d'accéder directement à l'auteur des faits et d'établir la preuve technique irréfragable de l'identité de l'auteur.

Le praticien est donc dans une situation paradoxale car l'exigence du juge est de plus en plus forte pour que les critères d'authenticité, d'intégrité et de traçabilité de la preuve soient respectés. En même temps, les coûts et les lenteurs des démarches permettent, le cas échéant, à la preuve électronique de s'échapper ou empêchent que son intégrité soit préservée.

IV.5. La dynamique de la preuve numérique dans l'expertise

David ZNATY : Président de la Compagnie des Experts agréés par la Cour de Cassation

Je souhaite rappeler en préalable quatre points importants. La théorie ou la technique utilisée par l'expert est-elle testable ou a-t-elle été testée ? Ont-elles été soumises à la critique des pairs ? Il convient de faire valider tout ce qu'on fait pour ne pas être contesté dans la démonstration de la preuve.

Quand nous sommes dans un système d'expertise numérique, nous avons affaire à des griefs, sans savoir s'il s'agit de causes, et devons déterminer une preuve. Il existe plusieurs types de preuve. La preuve démonstrative, ou structurée, est répétitive et n'est pas contestable. La preuve semi-démonstrative ou semi structurée nécessite l'intervention humaine pour apporter des éléments d'information au magistrat. Enfin, la preuve peut être non démonstrative.

Nous sommes dans un monde où la réplique se fait en temps réel et où tout se met à jour en temps réel. Les données

numériques sont très fugaces. Du fait de la dynamique des documents, la préservation des preuves est primordiale. Les organisations ont changé. Les entreprises vont aussi vite que les réseaux avec leur front-office et leur back office présents dans le monde entier. L'expert doit donc disposer d'une compétence extrêmement riche car l'univers technique est complexe.

A l'occasion d'une expertise, nous rencontrons des problèmes de temps de réponse, de contrefaçons, de dysfonctionnements, de mails contestés.... Lors d'une expertise, nous commençons par examiner les pièces litigieuses.

Deux cas de démonstration de la preuve peuvent être cités. Dans le cadre d'un projet, sur la preuve semi démonstrative par les pièces, très souvent, les parties se disputent en civil sur les coûts et les délais d'un projet et nous fournissent des documents. Nous devons alors être un expert technique, un expert du projet ou avoir un ensemble de compétences. En plus des éléments fournis par les parties, l'expert doit consulter un nombre important d'éléments pour déterminer à quel moment le litige a commencé et étayer sa théorie par de la bibliographie, de la méthode et de la logimétrie afin de ne pas être contesté par les avocats et pour que le magistrat dispose d'un dossier solide. Un autre élément concerne le problème de document. Lorsque l'expert parvient à décrypter un document, il doit expliquer comment il a procédé, ce qu'il n'a pas toujours envie de faire. Enfin, sur l'authenticité des e-mails, le problème n'est pas d'authentifier les mails mais des logiciels permettent de crypter tous les e-mails de manière aléatoire. Il est alors possible que l'huissier récupère des informations qui ne peuvent être traités par l'expert.

Lors d'une affaire, la mission consistait à donner un avis sur la réalité de l'importance des dysfonctionnements légaux. Les

dysfonctionnements étaient internationaux et nous sommes arrivés au constat de l'impossibilité de reconstituer la configuration. Les avocats ont alors accepté que l'expert interprète par des hypothèses les dysfonctionnements trouvés dans les pièces, comme s'il avait en face de lui la configuration. Il s'agit alors d'une preuve démonstratrice par les pièces.

En 1994, un document a été mis sous ESCROW et l'expertise me parvient en 2009 ou 2010 : le plastique qui contenait le CD-Rom s'est ouvert par la chaleur. Or ce CD-Rom contenait la preuve de ce qu'une des parties voulait démontrer en vue d'une expertise. Nous avons été obligés d'écarter ce scellé. Dans un autre cas de sauvegarde sur CD, l'huissier avait décrit toutes les opérations effectuées par l'expert pour constituer le CD. Un avocat m'a demandé de refaire les opérations et je n'ai pas obtenu le même résultat : nous avons donc dû écarter le CD car certaines étapes avaient été sautées.

Dans un cas pénal, l'expert doit connaître non pas la technique mais le protocole. Une jeune femme a été accusée d'avoir détruit tout le système complexe de son employeur. Le juge d'instruction avait l'impression que la femme ne possédait pas de compétences suffisamment solides en informatique et nous lui avons donc posé quelques questions. Nous avons vite constaté qu'elle ne pouvait pas avoir détruit le système.

Lors d'une AGE au Zénith, trois résolutions passent. Ceux qui ont voté contre la résolution ont mis en doute l'AGE. Les huissiers ont sauvegardé les serveurs et les boîtiers de vote et l'expert a pu démontrer, après un certain nombre d'investigations, que tous les boîtiers n'avaient pas pu être lus dans le laps de temps écoulés grâce au protocole et à la simulation.

Enfin, un trader était accusé de ventes intempestives d'actions boursières et se défendait en disant qu'il ne pouvait pas arrêter son ordinateur. Avec l'expert et la répétition du protocole en présence des parties, nous nous sommes rendu compte qu'une fonction du clavier n'avait pas été testée du point de vue de la sécurité et que le trader, s'appuyant sur le clavier, a initié la vente des actions.

L'expert doit exécuter ses missions avec un haut degré de technicité et une pédagogie importante ; il doit maîtriser la logimétrie et être perspicace dans le choix des tests, dans un environnement géographique international. Nous devons investir dans des systèmes complexes. La question du maintien du contradictoire se pose car je ne sais pas comment nous procéderons. Les coûts d'expertise risquent de devenir très importants car la reconstitution et l'environnement des tests deviendront des points critiques. L'expert doit toujours rester au fait de l'état de l'art.

IV.6. Débat avec la salle

Bernard DENIS-LAROQUE : Expert de Justice près la Cour d'Appel de Paris

L'exposé terminal remet en perspective tout le colloque. Durant les débats, on a eu l'impression que l'expert était en charge de tout du moment que l'adjectif électronique était accolé au terme de preuve. Or les experts, et plus généralement les scientifiques, ne peuvent entraîner la conviction, comme l'affirmait déjà Platon dans le Gorgias. Les experts apportent des éléments qui doivent être solides mais pas des preuves. A partir de ces éléments, la conviction est entraînée par les avocats dont c'est le métier et par

le juge. Ce n'est pas parce que la preuve est numérique qu'elle est entièrement l'affaire des experts.

Nathan HATTAB

Bien entendu, la preuve est avant tout l'affaire du juge. L'expert recolle les éléments d'information qui dans le cas présent sont numériques et répond aux questions qui lui sont posées. L'expert n'a pour ambition que d'éclairer le juge.

La nature numérique de l'information n'est pas pour autant complètement neutre. Comme l'a dit le juge David BENICHOU, l'expert est un intermédiaire qui traduit.

Un participant

Je suis interpellé par les propos de David Znaty sur le respect du fameux contradictoire. Ces travaux peuvent-ils être menés pendant des jours et des jours en contradictoire ? Quelle est la tolérance que nous pouvons imaginer aujourd'hui ?

Maître François-Pierre LANI

La position des avocats est assez claire. Les parties au litige peuvent convenir, de manière consensuelle, que, dans l'intérêt du dossier, il n'est pas nécessaire de procéder à l'ensemble des tests car les expertises peuvent sinon durer des années, du moins s'avérer très coûteuses et complexes. Il en est ainsi notamment lorsqu'il faut restaurer l'environnement technique tel qu'il existait au moment des faits, surtout quand les serveurs sont implantés dans le monde entier. Nous avons vécu, avec D. Znaty, une telle expérience. Il n'en demeure pas moins que cette recherche du consensus entre les parties est difficile. A défaut

d'accord, l'expert doit procéder à la restauration de l'environnement technique au moment des faits.

David ZNATY

Chaque expert a sa manière de faire respecter le contradictoire. En ce qui me concerne, quand il s'avère difficile d'avoir tous les moyens et tous les acteurs *in situ*, je procède souvent à un exercice de simulation en présence de tous les acteurs. Je ne dis jamais aux avocats de ne pas venir à une réunion d'expertise au civil. Le problème du contradictoire ne tient pas tellement au fait que les personnes soient présentes mais plus au fait que le déroulement correspond bien à ce que l'on voit.

David BILLARD

Avons-nous connaissance en France d'un outil commercial qui aurait été invalidé dans une expertise ?

David ZNATY

Les outils ont pour certains été certifiés par des organismes comme le FBI. Il n'existe pas aujourd'hui, à ma connaissance, quelqu'un pour dire que l'outil ne marchait pas. L'expert doit toutefois vérifier que l'outil fonctionne car il se peut que, en utilisant trois outils différents, les résultats diffèrent. Il convient alors de connaître les possibilités et de bien connaître l'outil. Nous devons donc nous former sur les outils et échanger entre nous toutes nos informations.

Serge MIGAYRON

Les outils sont très complexes car ils concentrent beaucoup de fonctionnalités. Chaque outil a ses avantages et ses

inconvenients. Face à une même question, les résultats peuvent différer d'un outil à l'autre en fonction de ses spécificités.

Il convient donc d'être extrêmement vigilant sur l'interprétation des résultats obtenus. Par exemple, le fait que les résultats obtenus diffèrent avec 2 outils différents, ne signifie pas que l'intégrité de l'objet a été modifiée.

David ZNATY

Nous rencontrerons prochainement un important problème lié aux supports. Aujourd'hui, nous ne parvenons pas à analyser certains supports qui ont pourtant donné lieu à des décisions de justice et qui pourront être analysés à l'avenir, notamment en matière de cryptage de données. Il se peut donc qu'un jour nous revenions sur des affaires. Dans cette optique, les scellées doivent être constitués de manière parfaite, notamment pour les disques durs.

David BENICHO

J'ai récemment mandaté une expertise pour voir, qui a exploité un certain nombre de disques durs avec FTK. J'ai ensuite exploité la copie de travail avec un autre outil et nous n'avons pas trouvé les mêmes résultats. La CNEJITA pourrait faire des tests et les résultats intéresseraient toute la communauté et la feraient progresser.

Serge MIGAYRON

Les logiciels ont des comportements qui peuvent varier d'un logiciel à l'autre mais aussi d'une version à l'autre. Il n'est pas possible de tester toutes les versions de tous les logiciels

possibles : La charge de travail générée par ces tests serait trop importante.

Nathan HATTAB

Il nous arrive au sein de la CNEJITA, de procéder à de tels tests et d'échanger sur la question entre experts lors de journées de formation. Il nous est déjà arrivé de procéder à des exposés sur des outils après les avoir testés. Mais nous ne disposons pas des moyens financiers et techniques d'un laboratoire de certification.

Nous échangeons aussi de façon permanente entre experts sur une liste privée CNEJITA-Liste, lorsque nous sommes confrontés à de telles questions sur nos expériences respectives en la matière.

V. Clôture du Colloque

V.1. Synthèse et perspectives

Madame Mélanie CLEMENT-FONTAINE, Maître de Conférences, Co-directeur du master NTIC Université de Versailles Saint Quentin en Yvelines, Membre du Laboratoire Dante

La dématérialisation de la preuve suit l'évolution constante de la dématérialisation des échanges comme en témoigne, par exemple la mise en place des dossiers numériques près la Cour de cassation. Beaucoup d'éléments ont été abordés aujourd'hui concernant la constitution de la preuve numérique et son exploitation. Ils ont porté sur les acteurs de la preuve numérique, mais aussi sur la question de l'identification et enfin, sur les aspects transfrontaliers de la preuve.

I. Cette après midi a permis d'exposer les embûches qui existent pour passer de l'existence d'un droit à sa reconnaissance par la justice en cas de litige. Il paraît tout à fait évident, que ce passage de l'existence à la reconnaissance, le justiciable ne pourrait le franchir seul. Il lui faut s'appuyer sur les hommes et femmes du métier à savoir les avocats, les conseillers juridiques, les huissiers et les experts. L'étude de la preuve numérique mêle en effet les questions juridiques aux questions techniques. Il est donc nécessaire que cette double compétence soit réunie soit par une et même personne soit grâce à la collaboration de plusieurs personnes. Nous avons eu un aperçu de l'enjeu de cette

collaboration entre juge, expert, avocat et huissier chacun remplissant une mission qui lui est propre.

Les difficultés techniques sont nombreuses. Concrètement, elles conduisent les avocats à constituer eux-mêmes les preuves lorsqu'avant l'avènement du numériques c'était leurs clients qui les apportaient. On a parlé, à ce titre, d'avocat inspecteur ou d'avocat détective. Bien souvent, les avocats ont recours à l'expert pour arriver à constituer cette preuve car cela demande un savoir faire, la maîtrise d'une méthode scientifique. Si le numérique permet de multiplier les moyens de preuve, la preuve dématérialisée est vulnérable en ce sens qu'elle est altérable et falsifiable. Elle est également plus ou moins dépendante de son environnement qu'il convient de maîtriser. Elle est par ailleurs effaçable, mais peut laisser des traces involontaires qu'il faut savoir débusquer. La recherche des preuves numériques se fait donc par étapes qui sont l'identification, la préservation, l'analyse, la production.

La collecte de preuve n'est pas une fin en soit, elle est utile qu'à condition d'être exploitable. Il est, par conséquent, de prendre soin de répondre aux exigences légales : la loyauté dans la collecte de la preuve, s'impose également le principe de proportionnalité, l'exigence d'imputabilité, d'intégrité de fiabilité, le respect de la vie privée et du secret des affaires..... L'outil numérique étant en perpétuelle évolution, l'appréciation de ces critères applicables à la preuve numérique mue également.

II. Une des grandes questions abordées aujourd'hui a porté également sur l'identification des personnes. Il a été souligné la tendance du législateur à mettre à la charge de la sphère privée l'obligation de conserver les informations susceptibles de permettre l'identification de personnes :

Ainsi, une peine d'emprisonnement est prévue par le Code des postes et des communications électroniques : pour les opérateurs qui ne respecteraient pas l'obligation de conserver des données techniques de connexion dans les conditions légales. De même, depuis la loi du 21 juin 2004 les fournisseurs d'accès Internet ou de fournisseur d'hébergement peuvent être sanctionnés pénalement s'ils ne conservent pas les moyens d'identification des internautes. Nous pourrions signaler encore pour exemple de la participation de la sphère privée dans la constitution de la preuve, les réflexions menées en matière de cybercriminalité. Il est aujourd'hui question de développer la participation des internautes au recueil de la preuve (plateforme Pharos).

III. Nous ne sommes évidemment pas les seuls en France à nous poser toutes ces questions. De plus, le numérique ne connaît pas de frontière si bien que le commerce électronique ou la cybercriminalité présente aisément des éléments d'extranéité. L'harmonisation des procédures des règles de preuve est un enjeu capital. Or si en matière de cybercriminalité les efforts vont en ce sens ainsi que cela nous a été exposé, en matière civile la situation est moins envieuse.

L'actuel conflit de la France aux Etats-Unis en témoigne. La divergence d'approche des deux pays en ce qui concerne l'obtention des preuves dans le procès civil est à l'origine du conflit. La procédure de discovery américaine permet à chaque partie, préalablement au procès, d'exiger de l'autre la production d'éléments de preuves entendus de façon extrêmement large qui comprend tous les éléments susceptibles de faciliter l'établissement de preuve, si bien que la demande des parties n'a pas à être ciblée. Cela concerne aussi bien la preuve papier que la preuve numérique. Une loi américaine de 2004 américaine entrée

en vigueur en 2006 a d'ailleurs permis de préciser les modalités de la recherche des preuves électroniques pour tenir compte de leurs spécificités. On parle d'e-discovery.

Par opposition, les règles de preuve en France ne permettent pas à une partie de forcer l'autre à lui fournir des éléments de preuves sans avoir recours au juge afin que ce dernier ordonne une mesure d'instruction à cet effet. Par ailleurs, il n'est possible d'exiger la communication d'un document qu'à condition d'en déterminer la nature et l'objet. Autrement dit il n'existe pas de système équivalent à la discovery permettant une pêche à la preuve généralisée.

La divergence des régimes pose problème chaque fois qu'il s'agit de régler un conflit entre une entreprise américaine et une partenaire établi sur le territoire français. Il s'agit alors de déterminer dans quelle mesure l'application extra territoriale de la discovery aux fins d'obtention de preuves situées sur le territoire français est possible. La France, par une application généralisée d'une loi de 1980, a mis en œuvre un système de blocage en vue de forcer les parties américaines à renoncer à la discovery afin de recourir à la Convention de la Haye sur l'obtention des preuves à l'étranger en matière civile ou commerciale. La France fournit ainsi un fondement juridique aux entreprises françaises pour leur permettre de se soustraire à la discovery. Pour autant, La Cour suprême des Etats-Unis a, malgré tout, continué à considérer que la discovery était applicable considérant que la Convention de la Haye était une simple exception en matière de preuve à l'étranger lors des affaires soumises aux juridictions américaines. Il faut prouver que l'application de la Convention est en l'espèce plus raisonnable. Pour échapper à la discovery, l'entreprise française doit établir l'existence de difficultés suffisantes. Or les parties françaises n'ont jusqu'à présent par réussi à prouver un risque réel

de poursuites pénales en application de la loi de blocage française qui aurait constitué une difficulté suffisante. Effectivement, jusqu'à une décision de la Cour de cassation du 12 décembre 2007, aucune sanction n'a été prononcée à l'encontre d'une société française pour violation de la loi de blocage.

Au-delà de ce conflit, qui conduit à une concurrence des juridictions, les différences fondamentales des deux systèmes juridiques posent des problèmes liés à la collecte des données personnelles. Lorsqu'une entreprise est dans l'obligation de transmettre tous les éléments susceptibles de permettre la constitution de la preuve à savoir les disques durs ou les messages des employés, il y a un risque de porter atteinte à la vie privée, au secret de la correspondance, à la loi informatique et libertés sur la protection des données personnelles. Le Comité consultatif des autorités nationales des Etats membres de l'Union européenne en charge de la protection des données à caractère personnel ainsi que la CNIL ont donc été conduits à émettre des recommandations afin de concilier la procédure de la discovery et les exigences communautaires en matière de protection des données personnelles. Une recommandation de la CNIL a été rendue le 23 juillet 2009 par laquelle la CNIL constate en premier lieu un "accroissement des dossiers concernant des transferts de données personnelles vers les Etats-Unis (...) en raison de procédure de Discovery devant des juridictions américaines". Quant au G29 il a rendu en ce sens un document sur "la procédure d'échange d'informations avant le procès dans le cadre des procédures civiles transfrontalières".

La preuve numérique n'a pas fini de faire parler d'elle. Sa place toujours grandissante dans les procès appelle une prise de conscience chez les justiciables quant à la nécessité de se pré

constituer des preuves sans attendre qu'un conflit éclate et aussi de savoir les conserver.

Mais ceci, je crois, fera l'objet d'une prochaine journée d'étude de la Compagnie Nationale des Experts que je remercie tout particulièrement pour ce colloque.

V.2. Clôture des travaux

Monsieur Nathan HATTAB, Président de la CNEJITA :

En tant qu'experts, nous avons l'obligation de nous maintenir à niveau pour être en mesure d'analyser et continuer à interpréter cette information numérique.

Cette information numérique impacte les différents acteurs, collaborateurs de l'œuvre de justice dans leur pratique quotidienne.

La complémentarité entre ces différents acteurs n'est pas discutable et l'expert y trouve toute sa place, ce qui me rassure. L'expert est l'interprète qui explique un certain nombre de choses. Il occupe une position non contestable aussi bien en amont que pendant l'expertise.

Sa démarche intellectuelle, sa connaissance des finesses du contradictoire et sa rigueur en termes de procédure garantissent la qualité de la collecte de l'information numérique. L'expert pose des questions et permet ainsi à l'avocat et à son

client de se positionner face à l'information qu'ils détiennent en leur donnant conscience de la véritable pertinence et de la véritable fiabilité des éléments dont ils disposent.

Face à l'évolution et à la place prépondérante du numérique dans nos expertises mais aussi dans nos pratiques avec les autres acteurs de l'œuvre de justice, je suis à la fois rassuré et conscient, voire préoccupé.

Je suis rassuré car l'expert a sa place, compte-tenu de la complexité des questions qui lui sont posées. Son approche scientifique le positionne en interprète.

Dans le même temps, je suis préoccupé de la tâche qui nous incombe et de la responsabilité qui nous revient.

La dématérialisation se généralise. Les magistrats, les huissiers et les avocats travaillent avec et dans le numérique. Leurs procédures se dématérialisent. Les réseaux privés se développent. Les clés de certifications nécessaires à l'authentification et à la préservation de l'intégrité de l'information se répandent de plus en plus. Nous aurons prochainement l'obligation de les utiliser.

CNEJITA
Siège Social : c/o CNCEJ 10 rue du Débarcadère
75852 Paris Cedex 17
www.cnejita.org