La preuve écrite électronique et le droit français.

Interprétation, manipulation et falsification des écrits électroniques : de nouveaux enjeux pour l'exercice de la justice.

M2 NTSI – Paris Ouest Nanterre

Retrouvez ce document sur www.e-juristes.org

21 Janvier 2010

Auteur :

Fabien KERBOUCI
fkerbouci <at> gmail.com

Mots-clefs : droit loi manipulation falsification blanchiment preuve écrit électronique faille juridique déloyal informatique instrumentalisation justice hacking

Sommaire

Introduction

On dit de l'informatique qu'elle envahit notre quotidien. C'est tout à fait exact, et l'on pourrait même ajouter que l'informatique envahit désormais les tribunaux.

Que les juges fassent leurs enquêtes de moralité sur Internet, que les écrits soient informatiques, que les comportements des justiciables soient de plus en plus liés aux nouvelles technologies… Tout cela est une réalité.

Mais peut-on se fier sans discernement à l'avis de l'expert ? La numérisation de nos activités n'est-elle pas sans risque pour le justiciable et les acteurs des services de la justice ?

Aussi paradoxal que cela puisse paraitre, l'écrit électronique ne peut-être simplement ramené à l'écrit papier. Le raisonnement juridique qui doit découler de l'appréhension des preuves écrites électroniques n'est incontestablement pas le même que celui que nous adoptons régulièrement, d'où le risque d'une insécurité juridique dans le traitement des contentieux.

Un premier volet, juridique et doctrinal, s'attache donc à décortiquer le raisonnement du juge dans son interprétation de la loi, et dans son appréhension des preuves écrites électroniques. Celle-ci est soumise à controverse puisque, selon les raisonnements adoptés, une preuve électronique aura, ou non, toute sa force probante.

Par ailleurs, la preuve écrite électronique est telle que de nouveaux risques émergent. Des risques renforcés par la nature même de l'écrit : falsification des preuves, blanchiment, usurpation d'identité, interprétations de mauvaise foi… Tout cela est grandement facilité par l'émergence des nouvelles technologies, qui font fi de toute considération juridique, et l'obsolescence des technologies plus anciennes, peu fiables voire non sécurisées.

Le deuxième volet de ce rapport présente les faiblesses des principales preuves électroniques aujourd'hui introduites devant les tribunaux : document texte, e-mail, SMS, et relevés d'appel. Toutes ces pièces électroniques sont faibles et vulnérables. Le risque que le juge rende, de bonne foi mais à tort, une décision injuste est, aujourd'hui, plus que réel.

Nous verrons, en détails, par quelles manipulations volontaires les parties d'un procès peuvent faire trainer les procédures, étouffer la partie adverse, renverser la charge de la preuve, ou produire injustement des effets juridiques.

I. De la preuve en général

I. 1. Rappel du principe de la liberté de la preuve

Pour convaincre du bon droit de leurs prétentions, les justiciables français disposent, de manière générale, d'une grande liberté dans la manière d'établir les preuves ou éléments de preuve qu'ils soumettent au juge.

C'est vrai en matière pénale, en matière commerciale, également en matière civile, même si la loi peut imposer sur la forme de la preuve en certains domaines. Ainsi la contravention ne se prouve que par le procès-verbal.

Si le principe est général dans ces domaines du droit, les différents objets pouvant constituer une preuve, eux, sont spécifiques. Notre droit positif prévoit différents régimes de preuves, modélisant le processus décisionnel que le juge doit entreprendre pour évaluer la pertinence et la force d'une preuve.

L'appréciation de la preuve repose sur trois concepts clefs, établis comme suit : la **recevabilité légale**, la **force probante** et la **valeur explicative**.

I. 2. La recevabilité légale de la preuve

Le juge accepte de prendre en considération un élément de preuve sous certaines conditions. La loi précise les conditions sous lesquelles les preuves sont administrées ou présentées au juge en différentes matières. C'est ce qu'on appelle, en droit, le « régime de la preuve ».

Ainsi, en matière civile, le régime de la preuve impose aux parties de s'échanger les pièces probantes qu'elles possèdent en vue de préparer l'instance du procès. Si elles ne le font pas de manière régulière, le juge peut décider qu'une pièce ne sera pas admissible en instance de procès (Art. 132 à 135 du Code de Procédure civile).

En matière pénale le juge peut prononcer l'annulation des pièces probantes illégalement formées par les services d'instruction.

Le juge ayant toute liberté pour apprécier les éléments qui lui sont soumis, on notera que la preuve est également recevable au regard de sa nécessité et de sa forme.

I. 3. La nécessité et la forme de la preuve

La nécessité de la preuve et de sa forme sont deux conditions qui permettent au juge de retenir, ou non, la preuve comme élément mettant en lumière tout ou partie de la vérité sur les faits allégués par celui qui la présente.

Dans les contentieux civils opposant des particuliers ou des commerçants, il faut qu'il y ait contradiction ou incertitude sur un fait présenté vrai pour que le recours à une preuve soit nécessaire. Si les parties s'accordent sur un fait dans leur récit, la preuve de ce fait n'est pas nécessaire.

Sur le plan pénal les éléments de preuve que peuvent apporter les parties mises en cause sont également libres, même si la loi impose que certaines infractions soient prouvées par des pièces spécifiques. Ainsi pour la plupart des contraventions (infractions légères) le procès-verbal dressé par un agent de la force publique fait preuve, tandis que, pour les infractions les plus graves, le juge pénal fera constituer les preuves par les services d'instruction judiciaire. Dans ce cas, les preuves peuvent être de toute nature.

Au pénal comme au civil les parties peuvent donc apporter librement leurs éléments de preuve. Les preuves apportées par les parties au procès sont d'ailleurs décisives au pénal lorsque l'affaire n'a pas fait l'objet d'une enquête approfondie.

Sur la forme de la preuve : celle-ci doit être valablement formée par sa matérialité et sa causalité. Sa matérialité est nécessaire, car la preuve ne saurait-être une simple intention ou une pensée. En revanche, le témoignage oral d'un tiers sous serment est une preuve imparfaite : l'oralité est un mode de preuve recevable.

La preuve doit également avoir un lien de causalité avec l'affaire. Sont exclues les preuves fondées sur un raisonnement par l'absurde ou surréalistes, comme la constatation de phénomènes paranormaux.

On ne peut également construire des preuves en vue de se dégager de ses responsabilités. Ainsi, un témoignage de bonne moralité, produit par soi n'est pas recevable.

Passé ces exclusions, une fois la preuve reçue, il revient au juge de l'utiliser au sein de son processus décisionnel. Il doit pour cela donner un sens à l'élément qui est présenté à lui puis en mesurer la « force probante ».

I. 4. La force probante et la valeur explicative de la preuve

Toutes les preuves ne se valent pas. En effet, la loi consacre une supériorité de certaines preuves sur d'autres et le juge peut donc arbitrer plus efficacement le conflit de preuves. La « force » d'une preuve est ainsi nommée « force probante de la preuve ».

La force probante est une valeur **subjective** de la preuve car elle tient à la nature de l'élément devant faire preuve selon qu'il s'agisse d'un simple témoignage, d'un aveu, d'un acte écrit ou numérique, signé ou non-signé, d'un procès-verbal, d'un acte notarié, etc.

Ainsi, le témoignage verbal d'un tiers peut être « très solide et bien détaillé » mais n'a pas autant de force probante qu'un acte notarié s'y opposant. Quand bien même l'acte notarié serait fortement moins descriptif, il a une autorité écrasante sur le témoignage oral (art. 1341 du Code civil).

La valeur explicative de la preuve, elle, est laissée à l'appréciation totale du juge qui décide souverainement, ou éclairé de l'avis d'un expert, si l'objet que forme la preuve est efficace pour l'argumentation qui lui est proposée. Il s'agit là de la valeur **objective** de la preuve, c'est celle qui occupe l'essentiel des débats et des temps d'audience lorsque l'on aborde la question des preuves.

Mais ne nous y trompons pas : la valeur objective de la preuve, son impact dans l'argumentation juridique, est subordonnée à sa valeur subjective en maintes circonstances.

II. La preuve électronique

II. 1. De l'écrit électronique en général

On l'aura donc compris ce n'est fondamentalement pas le support sur lequel se présente un élément qui fait sa valeur en tant que preuve. Un ensemble de paramètres juridiques plus abstraits guident l'appréciation du juge.

Malgré cela, l'écrit électronique a suscité bien des suspicions du fait de son apparente volatilité. Un écrit électronique peut-il constituer une preuve à part entière ?

Tout d'abord il faut rappeler ce qu'est une preuve par écrit au sens de la loi. L'article 1316 du Code civil stipule que la « 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. »

De là, il ressort que le législateur a pensé large en détachant la définition d'une preuve écrite de la condition de son support. La preuve écrite est ainsi une donnée **abstraite** et **résultat** de données concrètes (chiffres, lettres, symboles…). L'esprit de la loi incite le juge à raisonner *à fortiori* pour déterminer, dans l'avenir, ce qu'est une preuve écrite. Cette définition moderne de la preuve écrite inclut donc, bien évidemment, la preuve écrite électronique.

Nous verrons que, de cet article de loi et de sa rédaction littérale, nait une insécurité juridique qui peut poser problème au juge ou aux parties en instance de procès, notamment sur la question de la force probante de la preuve.

II. 2. La force probante de l'écrit électronique

Les juristes mettent en débat la valeur que doit avoir l'écrit électronique en tant que preuve ; les ingénieurs en informatique également s'interrogent sur la nécessité de concevoir des outils juridiquement fiables, aveu de la faiblesse juridique des outils numériques d'aujourd'hui.

Notre droit positif, lui, a déjà pris une position sur le sujet. En effet l'article 1316-3 du Code civil stipule que « l'écrit sur support électronique a la même force probante que l'écrit sur support papier ». Mais à deux conditions. L'article 1316-1 précise ces conditions :

« L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité. »

La première condition est donc que la personne à l'origine de l'écrit soit identifiable. La seconde condition impose que l'écrit soit conservé dans un espace sécurisé.

Le cas classique d'une demande d'engagement envoyée par mail, puis acceptée par retour de courrier vaut donc bien, en matière de preuve, un engagement manuscrit. Il faudra simplement que dans leurs échanges les parties aient été identifiables sur tous les écrits formant les actes, et que les pièces de ces échanges aient été conservées dans un espace dûment protégé. A ce titre, une boîte de messagerie protégée par mot de passe permet de présumer une garantie de l'intégrité des données.

Précisons, toutefois, que la signature écrite sur papier n'est pas de force équivalente à la simple apposition de noms et prénoms en bas d'un courrier électronique.

Un engagement électronique, pris sur la simple base de l'apposition du nom des personnes qui s'y engagent, n'a de valeur que si aucun écrit papier et signé, même imparfait, ne vient s'y opposer.

Pour avoir valeur de signature forte au même titre que celle sur papier, la signature électronique doit répondre à des conditions légales de sécurité (art. 1316-4 du Code civil et décrets afférents). Notre propos ne sera pas de traiter en détails de la signature électronique, mais d'aborder la conception d'ensemble.

Concrètement la signature électronique est réalisée par des logiciels informatiques utilisant des algorithmes cryptographiques. Elle permet d'assurer l'intégrité et l'authenticité des actes.

La signature électronique est réputée fiable jusqu'à preuve du contraire. La simple mise en doute de la fiabilité du procédé ne lève pas la présomption de fiabilité, il faudra apporter éléments très concrets pour tenir une position contraire.

Quoiqu'il en soit, l'enjeu de la signature électronique n'est que secondaire au regard des enjeux qui pèsent sur le domaine de la preuve écrite électronique.

III. De la conception de la preuve écrite électronique

III. 1. Notions fondamentales d'informatique

Il importe de bien visualiser comment est représenté un document en informatique pour comprendre que le législateur a négligé un point fondamental et source d'insécurité juridique sur la question de *l'interprétation* de la « suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles » que forme un écrit.

En effet, en informatique toute donnée est représentée par une suite de briques fondamentales que l'on appelle « octets ». Un octet est typiquement ce qu'a décrit le législateur, à savoir une suite de chiffres, une suite de 1 et de 0 (code binaire).

Mais, dans un fichier texte du type le plus simple, les octets ne sont pas affichés tels quels. Ils sont retranscrits par le logiciel, *Word* par exemple, pour former des caractères ayant une signification intelligible. En effet, en eux-mêmes, les octets (les nombres) ne signifient rien. Il faut leur **donner** du sens.

Ainsi, la suite de chiffres électroniquement écrits « 01100001 » se lit « a ». C'est le logiciel Bloc Notes de Windows qui se charge d'interpréter la correspondance à travers ce que l'on appelle une « table de correspondances ». La table dite « ASCII » est la table de correspondance la plus populaire pour transformer un code binaire en symboles alphabétiques.

La même suite de chiffres, « 01100001 », pourrait être interprétée tout à fait différemment dans un autre contexte ou par un autre outil.

Par exemple s'il s'agit d'un élément d'adresse IP alors la suite signifie « 141 » et non « a ». De même, s'il s'agit en informatique de représenter la couleur rouge, cela signifierait que le rouge est à 55% d'intensité.

Il faut retenir, qu'en informatique fondamentale, le sens donné à un codage électronique peut être radicalement divergent d'une analyse à l'autre, bien que les données brutes, elles, soient rigoureusement les mêmes. C'est, bien sûr, le contexte habituel d'utilisation de ces données qui permet de ne retenir qu'un seul choix de lecture pour celles-ci.

Il est toutefois des cas où l'on est obligé de travailler sur des écrits en employant plusieurs niveaux de lecture. Prenons le webmaster d'un site qui crée des pages web en code source HTML avec un logiciel spécialisé : le résultat produit de sa page web par le navigateur Internet n'est évidemment pas le même que le résultat produit par le logiciel d'édition spécialisé. Il n'existe pourtant qu'un seul et unique fichier.

Mais alors, à l'inverse d'un écrit papier, où l'on ne peut que s'interroger sur le sens des phrases, il est possible, en électronique, d'utiliser un même ensemble de données pour former des « phrases » complètement différentes, avant même de commencer à s'interroger sur leur sens propre.

L'information électronique porte donc **toujours** à des interprétations **équivoques**. Il faut au préalable définir une grille de lecture, un **système d'interprétation**, pour rendre l'information univoque.

De ce fait, le juge est entièrement dépendant de l'interprétation des données électroniques faite par les logiciels ou les experts. L'interprétation a un impact certain dans le processus décisionnel du juge et celle-ci est en réalité exercée par un tiers, chose ou personne, libre de toute contrainte légale.

Cette interprétation étant très technique, le juge non éclairé ne peut que difficilement en évaluer la qualité, et la pertinence. Cela le rend dépendant d'une source d'interprétation qu'il ne peut que présumer fiable.

Dans les cas où le magistrat fait appel à un expert judiciaire, il saura si l'écrit produit devant lui est fiable ou non. Alors, où est le fond du problème ? C'est que l'on oublierait presque que l'écrit électronique envahit notre quotidien : s'appuyer sur l'expertise judiciaire ne sera pas toujours possible.

III. 2. L'écrit électronique et son interprétation

Le sens intelligible de la preuve électronique est fondamentalement lié à l'interprétation qu'en rendent les logiciels. Si l'interprétation qui est faite des données est faussée, alors leurs significations intelligibles le seront également.

Par exemple, il est possible de retrouver dans les milliards de chiffres formés par le nombre Pi, une fois que ceux-ci sont écrits sur disque dur, des noms et des prénoms d'individus de notre entourage. Il suffit simplement d'interpréter les chiffres, non plus comme une séquence de nombres, mais comme une séquence de lettres.

A ce titre, on trouvera la marque « Coca » ou « Nike » dans le nombre Pi. Il serait toutefois absurde de considérer que la reproduction du nombre Pi constitue une atteinte du droit des marques.

En revanche la suspicion pourrait être de rigueur s'il s'agissait de constater ces noms de marque, non plus dans un nombre mathématique naturel, mais dans un fichier créé par une société concurrente…

En revanche, faire savoir que l'on a trouvé, dans Pi, le nom d'un de ses collègues étranger, ainsi qu'une injure raciste pouvant lui être imputé, est un autre problème juridique.

Lire un écrit informatique de manière volontairement biaisée, afin de lui donner un caractère préjudiciable, peut être condamné en fonction du préjudice (sur la base de diffamation par exemple). Mais donner un sens biaisé à une donnée électronique n'est pas illégal en soi.

Par analogie, lorsqu'un interprète traduit le discours d'un ambassadeur, il imprègne la traduction de ses propres impressions, mais aussi de ses propres erreurs. Il y a ainsi une infinité de variations possibles de la traduction des propos tenus par l'ambassadeur.

Prenons un dernier exemple d'interprétation biaisée des écrits informatiques : suite aux attentats du 11 Septembre 2001, on apprend, sur Internet, que l'un des avions s'étant écrasé à New York aurait porté comme nom de vol « Q33NY ».

Interprétée dans une police de caractères différente des polices européennes la chaine de caractères « Q33NY » donne sous la police Wingdings :

La rumeur se propagea alors sur Internet : des sociétés éditrices de logiciels seraient-elles en lien avec les terroristes ? Plus amusant encore : peut-on lire le futur dans l'informatique ? L'explication était plus triviale : il n'y a tout simplement jamais eu de vol nommé « Q33NY ». Il s'agissait d'un canular douteux.

Revenons au fond du sujet. Des exemples précédents nous comprenons que les significations, données aux écrits électroniques interprétés librement, peuvent être originales, fantaisistes ou préjudiciables.

En informatique la bonne interprétation du sens de données binaires présuppose **toujours** que l'on ait, entre la donnée brute et son sens intelligible, un **système d'interprétation** des données. Dans le cas de l'ambassadeur, et de son interprète, il s'agit du vocabulaire de la langue, de ses fonctions grammaticales, mais aussi de l'intellect propre à l'interprète.

En informatique ce système d'interprétation des données prend quasi exclusivement la forme d'un logiciel. Son fonctionnement est donc prédéterminé par nature : un logiciel, contrairement à un interprète, est fortement déterministe. Mais son utilisation, elle, ne l'est pas.

Il existe aussi des systèmes d'interprétation des données binaires faites pour l'homme, et utiles justement à ceux qui créent les logiciels. Il s'agit des standards informatiques et de la documentation industrielle.

La loi, elle, fait abstraction totale du fait que les informations électroniques ne soient pas directement intelligibles par l'homme, mais interprétées. Or, ces interprétations peuvent varier du tout au tout, en fonction de la volonté des personnes qui font, ou utilisent, les logiciels informatiques.

L'absence de prise en compte, par le législateur, de cette étape d'interprétation préalable fait que l'interprétation, rendue par le logiciel ou le technicien, n'est soumise à aucune contrainte légale.

Par extension, puisque la loi le permet, n'importe quel fragment de fichier, de quelque nature que ce soit, et pour peu qu'on puisse lui donner une signification particulière, peut être qualifié d'écrit électronique.

Ce vide juridique, volontaire ou non, crée des risques qui sont supportés à la fois par le justiciable, en tant que partie au procès, et par le magistrat, dans sa mission d'exercice de la justice.

III. 3. De l'interprétation juridique de l'écrit électronique

Il y a deux conceptions juridiques que l'on peut se faire d'une preuve écrite électronique au sens de l'article 1316 du Code civil : une conception idéaliste et une conception matérialiste. Traitons dans un premier temps de la conception consacrée par le législateur, la conception idéaliste de l'écrit électronique.

De la conception moderne de la loi le juge doit considérer une suite de nombres binaires, stockée sur disque dur, comme une simple « modalité de transmission » de l'écrit. Est considéré comme l'écrit le résultat **affiché sur l'écran** de l'interprétation des nombres binaires par un logiciel. Tout ce qui ne s'affiche pas sur l'écran ne saurait constituer un écrit.

Il faut donc traduire ce que « dit » le disque dur pour **produire** un écrit ayant un sens intelligible. C'est ce sens qui forme la preuve. Une suite de nombre binaires sur disque dur n'est donc pas, au sens légal du terme, un écrit: l'écrit et sa signification probante ne sont que le résultat d'une interprétation. C'est une **conception idéaliste** de la preuve écrite.

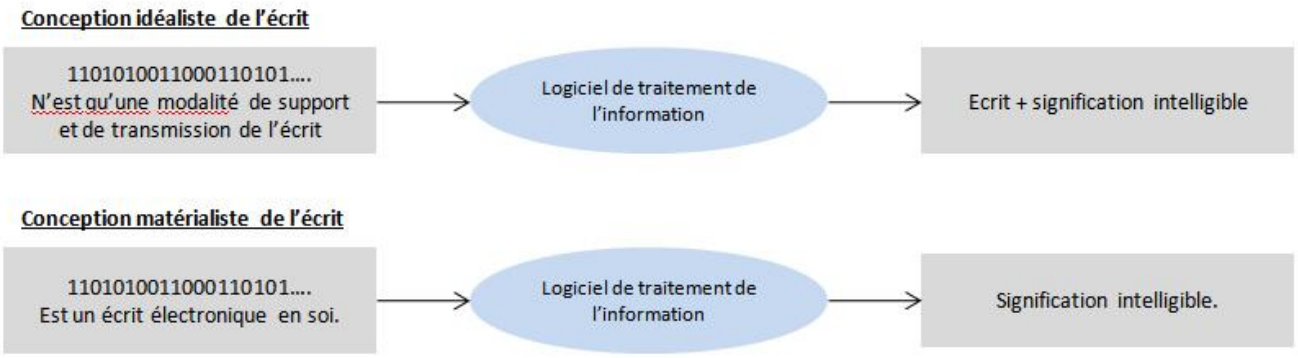
Une autre conception de la loi voudrait que le juge considère le disque dur et ce qui y est gravé comme un tout formant un écrit, toujours au sens légal du terme. Les modalités de transmission seraient alors définies comme les **actions humaines** réalisées pour transmettre les données, ainsi que les moyens temporaires employés pour fixer l'écrit (transmission par le réseau par exemple), le support étant alors l'ordinateur qui intègre le disque dur.

Comme précédemment, cet écrit devra être traduit pour pouvoir être rendu intelligible. Toutefois la transcription ne produira pas l'écrit, seulement son sens. C'est véritablement **une conception matérialiste** de la preuve écrite, très proche de la traditionnelle preuve écrite papier.

Par analogie on pourrait dire que le logiciel joue le rôle de la plume, le disque dur joue le rôle de papier, l'état du disque dur joue le rôle d'écrit au sens symbolique. Il faut néanmoins avoir l'esprit suffisamment moderne pour admettre qu'une série de transistors puisse constituer une suite de « symboles », comme l'exige la loi. Mais c'est aussi dans cette optique d'élargissement du concept de l'écrit que la loi a été conçue et donc, dans le respect de l'esprit des lois, **ces deux conceptions sont**

applicables en droit. Le hic ? Elles sont fondamentalement incompatibles, et leurs conséquences juridiques divergent radicalement.

Il y a ici une opposition entre la conception matérialiste et la vision idéaliste de la loi. Dans la conception idéaliste de la loi, l'écrit et son sens ne sont produits qu'après interprétation de données informatiques. Dans la conception matérialiste de la loi, l'écrit existe déjà en tant que tel et son interprétation ne fait que produire son sens (v. fig. 1).



(fig. 1) Deux raisonnements juridiques distincts pour interpréter l'écrit électronique

Or, nous allons le détailler par la suite, le choix idéologique de l'objet qui forme un écrit a des conséquences pratiques en droit.

Il est évident que l'on ne parle pas de la même chose selon que l'on dise que l'écrit est un disque dur, ou que l'écrit est ce qui s'affiche sur un écran. L'objet même qui porte la preuve est de nature différente et donc, en cas de conflit de preuves, le choix pourra paraitre cornélien. Et il le sera sûrement : aucune de ces conceptions ne convient vraiment à l'aube de l'ère numérique.

Si le juge, en face de cas concrets, n'utilise pas une approche différente de la loi il se heurtera, tôt ou tard, à de sérieuses difficultés d'interprétation des écrits électroniques. C'est sur ces difficultés que risquent de se construire les revirements de jurisprudence et l'insécurité juridique.

IV. Des faiblesses de la qualification juridique de l'écrit électronique

IV. 1. Faiblesse de la conception idéaliste de l'écrit électronique

Parlons tout d'abord des faiblesses de la conception idéaliste de l'écrit électronique, celle consacrée par la loi. Dans cette approche le juge ne retient pas la suite de nombres binaires comme étant un écrit mais le résultat de la transcription de cette suite, affichée sur l'écran, comme formant un écrit.

Les logiciels ne travaillent jamais qu'avec une partie des informations contenues dans les fichiers, et ne reproduisent que rarement à l'utilisateur l'intégralité des informations qui y sont contenues.

On perd des informations en focalisant son analyse sur le résultat d'une ou de deux transcriptions, tandis que l'objet duquel découle la transcription est, lui, complet.

Ainsi, à l'ouverture d'une page web par un navigateur Internet, les données de la page web seront traitées, exécutées, puis supprimées de la mémoire de l'ordinateur qui ne conservera que ce qui permettra l'affichage en couleurs de la page sur l'écran.

Or, c'est aussi sur la base de ces données temporaires ou inemployées par le logiciel que peuvent se fonder les prétentions des justiciables. Mais comment des informations aussi imperceptibles peuvent-elles fonder une preuve écrite ?

Mettons en scène deux travailleurs de bureaux : Bob et Alice. Lui et sa collègue sont en compétition pour une promotion à un poste de niveau hiérarchique plus élevé.

Cette rivalité a fait naître entre eux de nombreuses tensions et il est déjà arrivé qu'ils s'échangent verbalement quelques noms d'oiseaux. Ils évitent toutefois de le faire par écrit. Chacun sait que l'autre attend : l'arme imparable qui permettrait l'éviction rapide du concurrent, si ce n'est plus.

Malgré tout, bien obligés de travailler ensemble, leurs échanges électroniques restent courtois et professionnels. Mais un jour, Bob se voit donner l'obligation de préparer un rapport pour Alice. Il va donc rédiger son rapport, qui portera son nom en première page, et l'enregistre sous forme de fichier texte, comme fichier au format PDF.

Souhaitant se défouler quelque peu à l'occasion de cet envoi, mais trop lâche ou trop intelligent pour le faire ouvertement, l'auteur du rapport va glisser, au sein de son fichier PDF, une insulte gravement blessante à l'égard de sa collègue, tout en

s'assurant bien, qu'à l'ouverture du fichier par voie traditionnelle, l'on n'en constate nullement la présence.

En effet, dans les fichiers informatiques complexes, certaines zones inemployées par les fonctions avancées du logiciel peuvent être écrasées par des informations arbitraires, sans préjudice de la bonne lecture du document. C'est le cas des fichiers au format PDF ou DOC, mais aussi d'une pléthore d'autres formats de fichiers.

Comprenons bien : si le fichier est ouvert par la voie « usuelle », la phrase n'apparait pas. Et, si l'on ouvre le fichier avec un autre éditeur de texte, non compatible PDF, le contenu du fichier sera inintelligible à l'exception de la phrase « secrète » qui sera nettement lisible.

C'est ainsi qu'il remet à sa collègue ce rapport en PDF, sur CD-ROM. Le détail est d'importance, le CD-ROM étant un support intègre pour les données, au sens légal du terme.

Alice va chercher à ouvrir le fichier mais, par mégarde, avec un mauvais éditeur de texte. Elle voit alors l'injure blessante et, furieuse, avertit son employeur et décide au final d'engager une action en justice, au civil et au pénal. Amenons nos protagonistes au début du procès.

Pour sa défense Bob va maintenir qu'il est innocent. Il produit un témoignage écrit fait sur l'honneur, d'un tiers « complice », attestant ne pas l'avoir vu réaliser d'opération de ce type le jour de la transmission du fichier. Il explique aussi que, du fait que l'information soit volontairement cachée, elle ne pouvait être raisonnablement contrôlée par le propriétaire du fichier, c'est-à-dire lui. Enfin il affirme qu'il n'existe aucune preuve qui permette de l'identifier avec certitude comme auteur de l'insulte.

La partie adverse, elle, soutient que ces explications ne sont que vaines oralités, qu'il existe un écrit électronique insultant, transmis sur support intègre, qui porte explicitement le nom de son auteur. Toutes les conditions seraient réunies pour donner à cette pièce à conviction une valeur probante forte, supérieure même aux prétentions orales et témoignages douteux s'y opposant.

L'analyse première de la situation laisse à penser que l'accusation est en position de force dans le procès. Mais que va faire le juge qui raisonne en idéaliste de la preuve écrite électronique ?

Il va tout d'abord constater, par l'ouverture normale du fichier avec le logiciel Adobe Reader, que l'écrit électronique qui se présente à lui ne contient pas d'injure et que cet écrit, honnête, porte le nom de son auteur : Bob.

Puis, dans un second temps, il va ouvrir le fichier par une voie « anormale », avec un autre logiciel de texte. Il constate alors qu'il existe bien un **second** écrit électronique, insultant, mais que celui-ci est anonyme : le reste du document n'étant pas compris par le logiciel, le nom de son auteur n'apparait pas, ou pas de manière intelligible.

Ainsi le procédé d'interprétation des données qui met en lumière l'infraction ne permet pas de faire le lien avec son auteur, et le procédé d'interprétation qui identifie l'auteur du document ne permet pas faire le lien avec l'infraction. On dit de ces interprétations qu'elles sont **mutuellement exclusives** (« ou exclusif »).

Il n'y a donc pas **un** écrit résultant d'**une** interprétation des données électroniques mais bien **deux** écrits résultant de **deux** interprétations différentes de **mêmes** données électroniques.

Il en découle que la force probante de l'écrit, affirmée par Alice en accusation, ne tient plus vraiment en l'espèce, puisque l'écrit qui caractérise l'infraction, la preuve utile donc, ne remplit pas les conditions légales de preuve au sens de l'article 1316-1 du Code civil.

Pour avoir force probante au même titre que l'écrit papier, l'écrit électronique doit permettre d'identifier la personne dont il émane. Le juge, qui se voit donner par la loi toute liberté pour décider du sens des preuves, et assurer l'exercice d'une justice équitable, se trouve dans une situation délicate : l'écrit produisant l'injure ne permet pas, à lui seul, d'identifier son origine. En d'autres termes on dira que l'infraction n'est pas clairement réclamée par un individu identifiable.

Sur la base d'une conception idéaliste de la preuve écrite le droit pénal n'est pas applicable car on ne peut imputer un auteur à l'écrit formant l'infraction : il n'a pas d'origine **certaine**. Le doute pourrait donc primer en faveur de l'accusé.

En revanche, sur le plan civil, la donne est différente. L'article 1384 du Code civil explique ainsi : « on est responsable non seulement du dommage que l'on cause par son propre fait, mais encore de celui qui est causé par le fait des personnes dont on doit répondre, **ou des choses que l'on a sous sa garde**. »

Le rapport était sous la garde Bob, et celui-ci n'y a peut-être pas prêté suffisamment d'attention. Bob peut ainsi être astreint à compenser financièrement le préjudice moral causé par le texte qui a été inséré dans son fichier, et dont il est le gardien légal, donc le responsable civil.

Pour pouvoir faire condamner l'auteur de l'injure sur une base légale plus ferme, **le juge ne pourra pas tenir sur une conception idéaliste de l'écrit**, car de celle-ci découlent deux écrits bien distincts, qui, même liés par leur modalités de transmission, ne remplissent pas les mêmes conditions.

Le juge doit donc se rapprocher de la conception matérialiste de la loi où l'ensemble des données binaires du fichier seront vues comme un seul élément, un écrit à part entière, indivisible, et où l'ensemble des systèmes d'interprétations du document ne font que produire les différents sens sur lesquels le juge doit se prononcer.

Cette approche permettra d'opposer un écrit électronique unique à un autre écrit papier unique même s'il ressort de l'écrit électronique qu'il revêt plusieurs sens. Cela correspond à l'intuition que l'on pense devoir se faire du sujet. Malheureusement cette approche, elle aussi, ne va pas sans poser de problèmes juridiques…

IV. 2. Faiblesse de la conception matérialiste de l'écrit électronique

Dans une approche matérialiste de la preuve écrite, le juge reconnait directement à une suite de chiffres binaires le statut d'écrit électronique, au sens légal du terme.

Cela lui permet de ne plus travailler que sur les significations de l'écrit, et non sur une multitude d'écrits générés par des interprétations différentes des données.

Mais cette définition matérielle de l'écrit électronique ne va pas sans poser de problème car elle rend légalement acceptable l'idée qu'un fichier audio (WAV, MP3…) ou vidéo (AVI, MPG…) est un écrit électronique, ces fichiers étant par essence même des suites de chiffres (1 et 0) qui ne peuvent être rendus *intelligibles* que par un logiciel adéquat (lecteur audio/vidéo), exactement au même titre, ni plus ni moins, que les fichiers textes traditionnels. Il y a même des formats de fichiers hybrides qui mélangent vidéo, texte et images (ex : fichiers Adobe Flash au format SWF, jeux vidéo…).

Dans cette conception matérialiste la loi ne prévoit pas que le juge traite de manière différenciée les écrits électroniques selon leur **fonction**. Peu importe qu'ils représentent des fichiers textes, images, vidéo ou audio : tous ces modèles de données entrent dans la définition prévue par le législateur de « suite de chiffres ».

Dans une conception matérialiste, en refusant la définition d'un enregistrement audio numérisé sur ordinateur comme écrit électronique, le juge ne peut pas non plus légalement retenir la qualification d'une image JPG qui serait une photocopie numérique d'un document papier (scan). En effet, au même titre que le fichier audio, le fichier image doit être interprété pour pouvoir être rendu intelligible. Et tous deux rentrent parfaitement dans la définition d'écrit électronique.

Il est possible d'adopter une tierce position consistant à concilier ces deux approches. On qualifiera cette réflexion de conception en « poupées russes » de la

preuve écrite électronique. Dans cette approche le juge doit considérer que la suite de nombres binaires est un écrit électronique en soi, mais que cet écrit peut lui-même en véhiculer d'autres. Il peut ainsi exister un **emboitement des écrits**.

IV. 3. La conception en « poupées russes » de l'écrit électronique

Du fait de la complexité croissante du format des données informatiques, les limites inhérentes à l'écrit, telles qu'on les connaissait, volent en éclat.

L'une des caractéristiques fondamentales de l'informatique est qu'il est possible d'emboîter un fichier au sein d'un autre fichier, puis de répéter cette opération à l'infini. La répétition d'une opération de ce type est appelée « fonction récursive ».

En comparaison, dans notre univers matériel, il est impossible de « ranger » un écrit papier **dans** un autre écrit papier.

Tandis qu'un bloc de données informatique, lui, peut contenir d'autres données qui sont autonomes en elles-mêmes. L'écrit peut être incorporé au sein d'autres « écrits », plus larges, et de différentes natures.

Par exemple, la vidéo d'un mauvais plaisantin qui contient un sous-titrage falsifié, et reprenant d'ignobles propos diffamatoires, peut être caractérisée comme un fichier unique, véhiculant à la fois du texte écrit, une donnée audio et une donnée vidéo.

Au sens de la loi, et dans la conception idéaliste de l'écrit, le texte injurieux est bien un écrit électronique puisque suite de symboles. La vidéo se définira alors comme support de transmission. Mais, cette approche fait du contenant en lui-même un objet auquel le juriste n'aurait normalement pas à s'intéresser, et à tort.

Le support peut, en effet, également être la source de preuves tangibles, contenant des écrits, et permettant, par exemple, d'identifier leur auteur. Ce support s'il est lui-même lu comme vidéo ne signifie nullement qu'il ne contient *que* des informations vidéo. C'est le cas, par exemple, des bases de données.

Une base de données peut contenir des informations textes, audio, vidéo… La base de données pourrait être rattachée à la personne qui en émane si elle porte les informations de son créateur. De ce fait la base de données peut servir de preuve écrite quand bien même sa fonction principale n'est que de *contenir* d'autres données. C'est sur ce point que la loi du Code civil est faible : le législateur n'a pas

prévu que le « support » et les « modalités de transmission » puissent eux-mêmes être des écrits, en partie ou à part entière.

La précision aurait pu être aménagée de la sorte : si une origine commune peut être établie entre des écrits électroniques en apparence distincts, alors le juge pourrait décider de traiter ces écrits comme un seul. Cela vaudrait pour les écrits transmis en fragments ou tombant sous le coup de grilles de lectures différentes.

Et, par ailleurs, si le support ou les modalités de transmission d'un écrit électronique devant servir de preuve représentent, eux-mêmes, des écrits, alors ils pourront être assimilés en tant que tels, et avoir force probante.

Cette approche en « poupées russes » permet, au juge, d'aborder un document **ou un matériel**, à la fois comme écrit unique, mais aussi comme réceptacle d'écrits distincts, selon le niveau de lecture à pratiquer et les circonstances du contentieux.

Fondamentalement, ce cadre analytique consacre la liberté d'appréciation de ce que doit être un écrit électronique, sans vider de sa substance la définition même de l'écrit.

Dans le cas de Bob et Alice, le juge pourrait décider que les deux écrits, le rapport et l'insulte produits de manières différentes, sont issus d'une même source de données, représentée aux yeux des parties comme un fichier informatique unique.

Le juge en déduit que cet écrit remplit les conditions prévues par la loi pour avoir force de preuve écrite : l'écrit constate l'infraction mais également son origine, et a été transmis sur un support intègre.

C'est, par analogie, la même problématique qui se pose lorsque l'on établit une distinction juridique entre l'hébergeur et l'éditeur d'un site sur Internet.

La vision classique de l'hébergement en ligne veut que l'hébergeur soit celui qui fournisse le matériel et que l'éditeur soit celui qui fournisse le contenu.

Or, via les flux RSS et l'actualisation automatique des contenus des sites, un webmaster peut voir l'espace public de son site reproduire des informations illégales, rédigées par un internaute inconnu à l'autre bout du pays.

Le juge, qui doit retenir ou non la responsabilité du webmaster, qualifie alors ce dernier non plus « d'éditeur » mais « d'hébergeur ». Et à bon droit car, en faits juridiques, le webmaster a produit un nouvel espace d'hébergement au sein de son propre espace d'origine. Ce second espace d'hébergement permet, à d'autres éditeurs de contenus, de publier sur le site.

Ainsi le lien entre l'hébergement et l'édition n'est plus unilatéral et à sens unique, c'est un lien qui peut être **récursif,** car l'éditeur peut librement se promouvoir

hébergeur chez son propre hébergeur. Cela n'anéantit toutefois pas la responsabilité de l'hébergeur d'origine, qui peut, malgré tout, être tenu responsable des contenus enregistrés par ces « sous-hébergeurs ».

Si les raisonnements employés pour qualifier l'écrit électronique et travailler sur sa force probante sont différents, il va nous importer de comprendre que, même si la loi était suffisante, elle ne pourrait prévenir des risques juridiques inhérents à la nature même des documents électroniques.

V. La manipulation de la preuve électronique

V. 1. Introduction aux techniques de manipulation des preuves électroniques

Il convient de rappeler que la « manipulation », contrairement à la « falsification », ne vise pas à altérer l'écrit en substance, mais l'appréhension intellectuelle que l'on se fait de sa valeur probante. La preuve reste donc intègre et il ne s'agit nullement d'utiliser un faux. Les procédés décrits dans ce chapitre sont donc légaux.

Posons au préalable les deux axes sur lesquels se développent les principales techniques de manipulation de la preuve ainsi que leurs objectifs attendus. On distingue la manipulation informatique de la manipulation juridique.

La **manipulation informatique** se fait en amont. Elle vise à extraire, de données informatiques, des éléments de preuve allant dans le sens de l'argumentation de la partie intéressée. Elle peut se faire sur l'analyse des écrits en eux-mêmes, mais également sur les moyens de transmission et de stockage de ces preuves (audit des procédures de transmission et de stockage).

La **manipulation juridique** se fait en aval. Elle vise à donner une signification de droit aux éléments de preuve apportés par la manipulation informatique. L'idée est d'inverser par tout moyen légalement admissible la charge de la preuve, y compris les preuves rendues intelligibles par voie d'expertise judiciaire.

Il s'agit donc de réduire la valeur probante des écrits adverses, afin d'instiller chez le juge des doutes raisonnables, ou encore d'allonger les délais d'exécution des procédures judiciaires en complexifiant inutilement le débat.

On peut aussi « obliger » le juge ou les parties adverses à commander expertises et contre-expertises aux fins de repousser, autant que possible, la date du jugement définitif, ou étouffer financièrement l'adversaire.

V. 2. Scénario de manipulation informatique et juridique des écrits électroniques

La manipulation informatique des preuves électroniques consiste à prendre une preuve, ou ensemble de preuves, et à l'essorer de toute substance *significative* dans le but d'affermir la preuve ou, au contraire, d'en détériorer la force probante.

A ce titre, les données informatiques se prêtent fort bien au jeu de la manipulation des preuves. Pour rendre accessible notre propos sur ce sujet nous allons construire un scénario simple de la vie courante, mettant en scène Monsieur et Madame aux prémices de leurs procédures judiciaires.

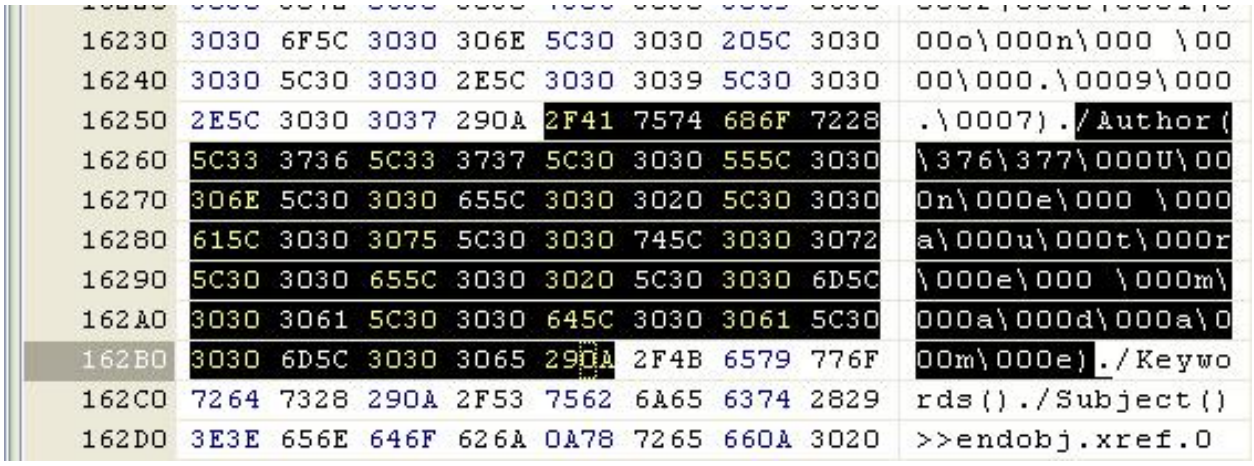
Ces deux personnes ne souhaitent plus communiquer oralement. Madame écrit donc à Monsieur, par voie de messagerie électronique exclusivement, pour lui faire parvenir une pièce jointe au format PDF. Ce fichier PDF est une lettre de mise en demeure à bon droit, peu importe la raison, et mentionne le nom de son auteur, c'est-à-dire de Madame.

Monsieur confirme à Madame la bonne réception du courrier et de sa lecture, mais fait savoir qu'il n'y donnera pas suite car il « doute de l'identité réelle de son auteur ». Quelque peu provoquant, il ne donne pas plus d'explication ni même de formule de politesse.

Furieuse, et sans autre demande d'information devant un acte de telle mauvaise foi, Madame assigne Monsieur en justice et produit l'e-mail envoyé ainsi que la réponse « de mauvaise foi » qui lui est parvenue. La justice demande alors à Monsieur de produire les éléments qui lui permettent de contester l'authenticité du courrier. En effet, celui-ci émane manifestement de Madame : à la lecture du PDF le nom de Madame apparait bien et a été envoyé, de surcroît, par l'adresse e-mail de Madame qui est bien connue de son destinataire.

Monsieur explique alors, qu'en ouvrant le fichier PDF avec un logiciel spécialisé, il s'est aperçu que le nom de l'auteur du fichier était tout autre que celui de Madame !

Le logiciel de création de fichiers PDF a en effet marqué le fichier avec un nom d'auteur différent de celui de Madame, et cette dernière ayant utilisé le logiciel sur l'ordinateur d'une collègue de travail, c'est le nom de cette personne qui apparait comme étant l'auteur du fichier. Evidemment Monsieur ne connait pas cette collègue…



16230	3030	6F5C	3030	306E	5C30	3030	205C	3030	00o\000n\000 \00
16240	3030	5C30	3030	2E5C	3030	3039	5C30	3030	00\000.\0009\000
16250	2E5C	3030	3037	290A	2F41	7574	686F	7228	.\0007)./Author(
16260	5C33	3736	5C33	3737	5C30	3030	555C	3030	\376\377\000U\00
16270	306E	5C30	3030	655C	3030	3020	5C30	3030	0n\000e\000 \000
16280	615C	3030	3075	5C30	3030	745C	3030	3072	a\000u\000t\000r
16290	5C30	3030	655C	3030	3020	5C30	3030	6D5C	\000e\000 \000m\
162A0	3030	3061	5C30	3030	645C	3030	3061	5C30	000a\000d\000a\0
162B0	3030	6D5C	3030	3065	290A	2F4B	6579	776F	00m\000e)./Keywo
162C0	7264	7328	290A	2F53	7562	6A65	6374	2829	rds()./Subject()
162D0	3E3E	656E	646F	626A	0A78	7265	660A	3020	>>endobj.xref.0

(Fig. 2) Extrait de fichier PDF lu avec un logiciel spécialisé

Ainsi, sur cette figure 2 apparait, à la colonne de droite, la mention du nom de l'auteur qui est générée par le logiciel ayant enregistré le document.

Le contenu est difficilement lisible pour le novice à cause de l'encodage dit « Unicode », mais si l'on ne prend que les lettres du bloc concerné, à droite, il est clairement écrit : « Author(Une autre madame)». Le fichier PDF ne véhicule donc pas d'informations sur un, mais sur deux auteurs bien différenciés.

On constate un écart, ou plutôt un gouffre, entre la perception des informations contenues dans un fichier et le contenu réellement véhiculé par ce même fichier. C'est sur cet écart que se fait la manipulation de la preuve.

Si nous revenons à notre cas d'école, que va décider le juge amené à statuer sur l'affaire ?

Tout d'abord, s'il manque de compétences techniques en la matière, il commandera une expertise judiciaire afin d'avoir quelques lumières sur la question. Il y a déjà, ici, allongement du délai de procédure.

De lui-même, et éventuellement aux termes d'une expertise, le juge devrait conclure que cet argument n'est pas suffisant pour ôter la présomption quant à l'auteur à l'origine du courrier.

Monsieur doit donc, au préalable, renforcer sa défense et c'est ce qu'il va faire en expliquant qu'il a également eu un doute quant à la nature du courrier électronique, en ayant constaté un changement dans l'adresse Internet IP de la personne qui l'émet.

En effet, si l'adresse électronique (adresse e-mail) de la personne à l'origine du courrier est bien la même, en revanche, le lieu d'émission du courrier, identifié par adresse IP, peut avoir changé.

Pour deux raisons essentiellement : soit la personne s'est connectée sur un réseau informatique autre que celui qu'elle utilise habituellement, soit le prestataire de courrier a opéré des modifications sur les machines susceptibles de relayer les courriers.

Dans les deux cas l'adresse Internet de la machine à l'origine de l'envoi ou du transfert des courriers peut avoir subi des modifications. Ce constat relève de l'audit des procédés et moyens de transmission.

Les adresses IP ainsi que beaucoup d'autres informations sont véhiculées dans les courriers électroniques en plus des informations traditionnelles créées par leurs expéditeurs. Elles permettent d'assurer la *traçabilité* du courrier mais fournissent aussi des pistes permettant de vérifier, en partie, l'authenticité d'un courrier.

Les ingénieurs en informatique appellent cette remontée d'information, sur un courrier électronique, une « analyse d'en-tête SMTP / *SMTP header analysis* » ; SMTP étant le nom du protocole de messagerie de référence sur Internet.

```
Delivered-To: destinataire@courrier.com
Received: by 10.213.7.5 with SMTP id b5cs30201ebb;
        Sat, 7 Nov 2009 08:44:09 -0800 (PST)
Return-Path: <expediteur@email.com>
Received: from mr.email.com ([10.213.26.140])
        by 10.213.26.140 with SMTP id e12mr971483ebc.0.1250002249048
(num_hops = 1);
        Sat, 07 Nov 2009 08:44:09 -0800 (PST)
Received: by 10.213.26.140 with SMTP id e12mr971483ebc.0.1250002249040; Sat,
       07 Nov 2009 08:44:09 -0800 (PST)
Date: Sat, 7 Nov 2009 17:44:08 +0100
Subject: Sujet de mon mail
From: Expediteur <expediteur@email.com>
To: destinataire@courrier.com

(…)
```

(Fig 3) en-tête SMTP, en rouge les informations d'adresses IP

Le juge entend donc que l'adresse IP de l'expéditeur des courriers électroniques a changé, et que le nom de l'auteur, enregistré par le logiciel de création de fichier PDF, ne correspond pas au nom de l'auteur affirmé dans le courrier. On pourrait croire que Monsieur avait effectivement des raisons valables de douter de l'authenticité du courrier électronique, d'autant plus que, dans d'autres cas,

notamment ceux proches de la cybercriminalité, ces éléments pourraient être parfaitement justifiés.

Monsieur pourrait enfoncer le clou en affirmant qu'il est de notoriété publique que le protocole de messagerie Internet traditionnel SMTP n'est pas sécurisé, qu'il se prête avec facilité à des fraudes, et qu'en conséquence le motif de son refus était parfaitement légitime et de surcroît motivé par les éléments de preuve apportés. Ainsi Madame n'aurait eu qu'à lui faire parvenir une lettre recommandée signée de sa main afin d'éviter tout malentendu.

Le jugement peut basculer en faveur de Monsieur : même astreint par le juge à l'exécution de la mise en demeure, le délai d'exécution de celle-ci pourrait se faire *à compter de la date du jugement* et non de la date de réception de la mise en demeure, contrairement à ce que prévoient certaines dispositions civiles ou commerciales (ex. article 1153 alinéa 3 et 4 du Code civil : les intérêts moratoires « ne sont dus que du jour de la sommation de payer »). En outre il ne serait pas tenu au règlement des dépens de la partie adverse.

V. 3. Autres techniques de manipulation des preuves

En manipulant la preuve à outrance, afin d'appuyer une position de mauvaise foi, on peut contourner certaines règles de droit en toute légalité.

Dans l'exemple précédent, l'objectif pour Monsieur était de gagner du temps sans préjudice de paiement d'intérêts.

Ne faisons toutefois pas passer le juge pour un ignorant de ces petites choses de l'informatique. La réalité est que, si le cas présenté ici est simple, et ne trompera peut-être pas en l'état, les cas « réels », eux, peuvent-être beaucoup plus complexes.

Les parties peuvent produire en justice, par extension abusive, des centaines de documents ou écrits informatiques induisant pour chacun d'entre eux deux ou trois grilles de lectures distinctes.

On notera donc qu'il existe une brochette de techniques de manipulation des preuves écrites électroniques :

- La réfutation de l'intégrité des espaces de stockage et de transmission (audit de sécurité) ;

- La déconstruction en multiples d'un écrit qui avait l'apparence d'être unique, puis l'attaque de la valeur probante de chacun de ces écrits (« division et conquête ») ;

- La démonstration de la modification du document par un tiers (audit des métadonnées) ;

- La réfutation de l'authenticité de l'acte sur la base des dates tampons générées par les systèmes informatiques (audit des chronologies) ;

- La démonstration de l'incomplétude des écrits (supposition de pièces manquantes, données boguées) ;

- La démonstration d'une volonté de nuire par l'écrit (ex : écrit contenant des données binaires assimilables à un virus et dont les alertes seront produites par un système antivirus spécialement choisi à cet effet)

Le principe, de la preuve écrite électronique ayant même force probante que la preuve papier, s'en trouve sérieusement mis à mal : on peut trop facilement « diffamer » l'écrit électronique en tant que preuve.

Tout cela ne serait pas si grave si, en sus, les quatre catégories d'écrits électroniques les plus produits par les justiciables français n'étaient pas également les plus facilement falsifiables.

Nous parlons bien sûr des **documents numériques**, des **e-mails** et des **SMS et appels téléphoniques**.

VI. La falsification des preuves électroniques

VI. 1. De la falsification en général

Rappelons, à toutes fins utiles, qu'aux termes de l'article 441-1 du Code pénal : « Constitue un faux toute altération frauduleuse de la vérité, de nature à causer un préjudice et accomplie par quelque moyen que ce soit, dans un écrit ou tout autre support d'expression de la pensée qui a pour objet ou qui peut avoir pour effet d'établir la preuve d'un droit ou d'un fait ayant des conséquences juridiques.

Le faux et l'usage de faux sont punis de trois ans d'emprisonnement et de 45000 euros d'amende. »

Ainsi, le fait de falsifier ne constitue pas une infraction en soi : il faut que la falsification ait vocation à porter préjudice, ou à produire des effets de droit qui n'auraient pu être produits en l'absence de falsification.

Il y a quelques facteurs dans l'univers numérique qui rendent faciles la production de faux ayant l'apparence manifeste de vrais. Mais, avant de parler de ces facteurs, distinguons au préalable la falsification d'une preuve **à posteriori** de sa falsification **ex nihilo***.*

La falsification *à posteriori* d'une preuve consiste à modifier un écrit existant et authentique afin d'en altérer le contenu, d'y supprimer des informations ou d'en ajouter de nouvelles.

La falsification *ex nihilo* consiste à produire une fausse preuve sans partir d'un écrit original. La distinction est importante car ces deux falsifications ne visent pas aux mêmes objectifs.

Si la preuve électronique est faussée *à posteriori,* alors la démarche de son auteur de modifier ou d'altérer la preuve est une démarche **préventive**, visant à se soustraire d'éventuelles poursuites judiciaires. Elle est généralement pratiquée à l'occasion d'un concours d'infractions plus graves (ex : piratage informatique, détournement de fonds).

Si la preuve électronique est créée *ex nihilo,* c'est au contraire qu'elle a pour but de faire produire des effets de droit à l'avantage de leur auteur. Il s'agit d'**instrumentaliser** les écrits falsifiés à des fins actives.

VI. 2. De la falsification des fichiers informatiques

Contrairement à un écrit papier, la modification en informatique d'un fichier n'entraine pas modification apparente des autres données contenues dans ce fichier.

Par exemple, si l'on inscrit une ligne entre deux paragraphes sur un acte papier, l'ajout apparaitra manifeste car l'esthétique et la présentation du document s'en trouvent altérées. Le papier lui-même subit la trace matérielle de l'écrit.

Si l'on reproduit la preuve papier pour masquer cet ajout on perd toutes les informations originales et il faut tenter de les reproduire au mieux (ex : cachet de la société, papiers carbones, etc.).

En revanche, ajouter une ligne entre deux blocs de données en informatique n'entraine pas modification des autres données et le fichier va s'adapter en taille et en apparence. Si le fichier contenait des images celles-ci seront conservées sans nulle détérioration.

Les *hackers* qui, après avoir piraté un système, « blanchissent » les traces de leur passage ne font que modifier des informations de journaux informatiques dans lesquels sont conservées les traces de l'activité du système, et des actions des utilisateurs. Les preuves doivent sembler fiables aux yeux des experts.

Une opération de ce type prend entre 10 minutes et une heure et ne laisse normalement pas de trace visible. Les fichiers de preuves, eux-mêmes, n'ont été entre temps ni déplacés, ni supprimés. Une telle opération de blanchiment serait inenvisageable sur des journaux d'événements imprimés sur papier, et rangés dans une armoire.

Un autre facteur, qui rend facile la falsification de preuves électroniques, tient en ce que les copies de fichiers informatique sont toujours d'exactes répliques des originaux. Il ne peut y avoir de détérioration de l'information, que le fichier soit copié une fois ou mille fois. C'est ainsi le rôle de nombreux protocoles Internet de s'assurer que les données sont transmises sans erreurs et à l'identique.

De fait, la copie d'un écrit en vue de le falsifier puis de remplacer l'original n'entraine pas détérioration des données, à l'inverse d'une photocopie ou d'un scan numérique.

De plus, le propriétaire du fichier copié n'étant pas dépossédé de son bien cela laisse au fraudeur tout le temps nécessaire à la falsification des écrits en vue de leur substitution ultérieure.

Reproduire ou falsifier une preuve ne laisse ainsi pas de trace matérielle apparente au sens propre du terme, et les analystes ne peuvent que s'appuyer sur l'apparence des données pour élaborer leurs conclusions.

Pour constater des traces matérielles, il existe des services spécialisés dans le recouvrement de données. L'analyse porte alors sur les disques durs, clefs USB, etc. aux fins d'en déduire les actions entreprises par les fraudeurs. Mais, là encore, si le fraudeur est suffisamment compétent il pourra échapper à ces techniques d'investigation (parfois si coûteuses qu'elles ne sont réalisées que pour des cas absolument nécessaires).

VI. 3. De la falsification des e-mails

L'e-mail est le moyen de communication le plus employé sur la planète, bien que les publicités abusives forment également l'immense majorité des courriers du web.

L'e-mail est présent à tous les niveaux de nos échanges en société : inscriptions sur des sites web, demande d'informations auprès d'un organisme, transmission de devis, échanges personnels ou entre collaborateurs au travail…

L'e-mail est devenu si important qu'il était normal que le législateur consacre l'écrit électronique, que peut former un e-mail, comme preuve valable des intentions et actes de personnes.

Le problème est que la messagerie électronique s'appuie sur un médium de communication (dit « protocole SMTP ») qui n'est pas fiable.

En fait, dire qu'aujourd'hui le système d'échanges de courriers est une passoire serait sous-estimer la gravité du problème. Car, dans ce système d'échange des données, n'importe qui peut se faire passer pour n'importe qui, et même antidater les courriers. Enfin notons que les courriers ne sont pas protégés par un cryptage.

En utilisant un serveur de messagerie sous contrôle le fraudeur peut réaliser des courriers qui usurpent :

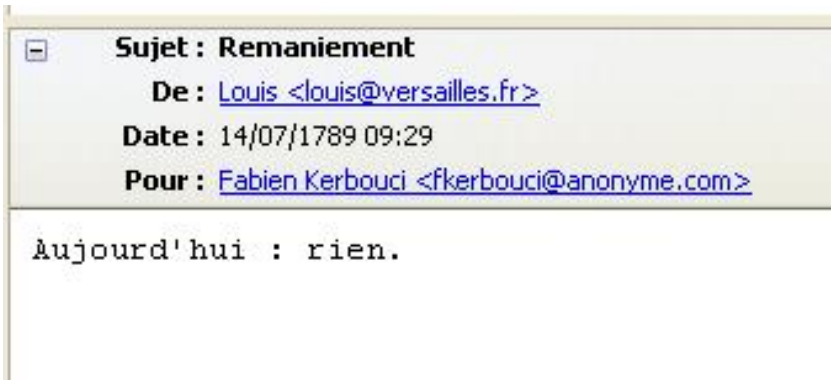
- L'adresse e-mail « From » de l'expéditeur, son nom et prénom

- La date « Date » d'envoi du courrier (il est même parfois possible de ne mettre que du texte, comme « Pas de date » - c'est dire si le système est permissif)

- L'adresse « To » qui permet de modifier l'adresse apparente du destinataire ; cela permet de faire parvenir un courrier de manière non explicite.

- L'adresse « Reply-To » de réponse au courrier (pratique pour pouvoir établir de vrais échanges en usurpant une fausse identité)

- Les données en en-tête pour la traçabilité et le relai des courriers. Avec ce bémol que, si les en-têtes sont falsifiés au départ, ils contiendront tout de même quelques informations authentiques (dates, IP…) ajoutées par les systèmes relais légitimes en aval de la livraison.



(Fig. 4) Un mystérieux e-mail manifestement falsifié et antidaté…

Notons aussi que les courriers électroniques sont archivés sous forme de fichiers en texte brut par les serveurs de messagerie.

Ainsi n'importe quel administrateur de système en entreprise peut insérer un courrier frauduleux au sein de ces bases de courriers. Lorsque le propriétaire de la base relève sa messagerie il verra apparaitre ce courrier falsifié.

Dans ce cas, le seul moyen permettant de démontrer que le courrier n'a jamais été envoyé consiste à remonter les en-têtes contenant l'adresse des serveurs relais puis de vérifier auprès de ces serveurs relais si un courrier a été transmis. Cela suppose donc une démarche effectuée par la police judiciaire ou l'instruction.

Un employé, de bonne foi, pourrait ainsi produire un courrier falsifié en justice, comme « preuve écrite », entrainant alors un jugement erroné, à moins que le juge, l'expert ou la partie adverse, n'envisagent ce cas de figure.

VI. 4. De la falsification des SMS et appels téléphoniques

Il est important de rappeler que le SMS et l'appel téléphonique peuvent constituer des écrits électroniques ayant force probante.

En ce qui concerne le SMS, il se prête tout à fait au rôle de preuve écrite électronique : c'est un document numérique qui identifie son expéditeur, son destinataire et qui est enregistré sur téléphone, donc un système présumé intègre.

En ce qui concerne l'appel téléphonique, il ne constitue pas une preuve écrite en soi. Mais l'enregistrement des numéros des appels entrants et sortants, ainsi que la date de ces appels, peuvent constituer des débuts de preuve (visant par exemple à prouver qu'une démarche particulière a été entreprise auprès d'un tiers).

Le problème c'est que l'un, comme l'autre, sont falsifiables de toutes pièces tandis que les mécanismes de protection sont quasiment inexistants.

En ce qui concerne la falsification des SMS, il faut savoir qu'elle n'est pas à la porté de tout le monde, mais presque. N'importe quelle société ayant droit d'accès à ce que l'on appelle un « service de routage de SMS » peut injecter sur le réseau téléphonique des SMS fabriqués de toutes pièces.

Il est ainsi possible de falsifier le numéro de l'expéditeur du message et d'accompagner le SMS d'un contenu préjudiciable. On peut même mettre du texte brut en tant que numéro. Des pirates informatiques, ayant déjà eu accès à ce type de service, ont pu injecter sur le réseau téléphonique des SMS falsifiés de toutes pièces. Cela s'appelle du « *SMS spoofing* ».

Etant donné que les requêtes sur les réseaux téléphoniques sont hautement falsifiables, et les protections quasi-inexistantes, le risque qu'un faux SMS puisse être produit devant la justice est bien réel.

Précisons également d'autres choses qui sont d'intérêt sur la question :

- Les SMS envoyés par téléphone sont massivement relayés par Internet et sur les réseaux des opérateurs privés, non par la voie des airs - sauf à l'expédition.

- Les SMS relayés sur Internet passent par des systèmes qui les enregistrent en clair et qui indiquent : le numéro de l'expéditeur, du destinataire, la date d'envoi et le contenu du message. Par expérience, nous savons que, dans certaines sociétés, ces SMS sont lus en toute indiscrétion par des employés ayant du temps libre et les droits d'accès nécessaires.

- Les formats des SMS sont variés (SMS simple, Flash SMS, MMS…) et il existe même des types de SMS qui permettent de télécharger l'intégralité du répertoire téléphonique contenu dans une carte SIM (*SIM Data Download*). C'est normalement une opération réservée au seul opérateur du client.

Le SMS apparait donc comme un moyen de communication hautement vulnérable, et ce en raison de l'inertie totale des opérateurs téléphoniques sur cette technologie largement dépassée, mais qui rapporte…

Pour ce qui concerne les appels téléphoniques, nous serons plus brefs. Il faut simplement noter que, lorsque l'on passe un appel, le numéro de l'appelant est envoyé sur le réseau téléphonique à la composition du numéro.

Or, ce numéro peut être falsifié. C'est une technique de mascarade que l'on nomme « *Caller ID Spoofing* ». Elle est réalisable avec quelques connaissances, du matériel et des logiciels spécialisés accessibles au grand public (pour simplifier un ordinateur suffit).

Aujourd'hui des organisations proposent à n'importe qui, moyennant commission, de passer des appels téléphoniques ou d'envoyer des SMS falsifiant les informations de leur émetteur. Les pages d'accès à ces services sont renvoyées par Google en premier résultat sur la base de quelques mots clefs.

Rappelons, qu'en eux-mêmes, les falsifications de SMS ou de numéros appelants ne sont pas des délits. Il faut que la falsification ait caractère préjudiciable pour constituer une infraction. De ce fait, le droit à l'anonymat peut s'exercer en ces domaines.

VI. 5. La falsification et le droit

Il n'est pas véritablement nécessaire de rappeler les règles de droit qui s'appliquent à la falsification. Traitons plutôt des problèmes auxquels le magistrat se trouve confronté face à la fraude et à la falsification des écrits électroniques.

Juridiquement, ces problèmes reposent sur deux constats : une forte dilution des faux dans l'immense majorité des écrits authentiques, et la complexité des écrits en eux-mêmes.

Premier point : l'immense majorité des écrits électroniques produits en justice sont honnêtes et non falsifiés. De ce fait, il est beaucoup plus difficile pour le magistrat de repérer par avance les écrits qui auront pu être falsifiés, ceux-ci étant noyés dans une masse d'écrits authentiques.

Bien sûr, la contestation de l'écrit par la partie adverse peut mettre la puce à l'oreille du juge, mais il est aussi des cas où l'écrit n'est pas directement imputable à un tiers partie du procès, alors personne ne viendra faire contestation.

Deuxième point : la complexité des écrits électroniques fait peser un risque sur les parties les plus démunies. En effet, le fait de falsifier un écrit va renverser la charge de la preuve sur la partie adverse, qui devra donc **prouver** par tout moyen que l'écrit qu'on lui impute n'est pas de son fait.

Au pénal, en procédure d'instruction, il est facile pour le juge de procéder à une vérification des écrits puisque cette vérification va entrer dans le cadre d'un grand

nombre d'autres procédures. Mais, en matière civile les preuves sont à la charge des parties.

De ce fait, la possible instrumentalisation déloyale de la justice française est aujourd'hui une menace bien réelle, et facilitée par l'avènement du tout numérique.

On pourrait qualifier l'ensemble des techniques et méthodes visant à instrumentaliser la justice à des fins déloyales « d'ingénierie judiciaire » - ce terme se rapprochant de celui « d'ingénierie sociale », qui est un ensemble de techniques d'usurpation de l'identité et d'abus de confiance, à des fins d'extorsion.

VI. 6. La sécurité des écrits électroniques

S'il est nécessaire de tirer la sonnette d'alarme, il est aussi important de rappeler qu'il existe déjà des solutions de sécurité, qui comblent certaines faiblesses exposées ici.

Par exemple, en ce qui concerne la sécurité des écrits et des preuves, il existe des logiciels permettant de vérifier si ceux-ci ont été modifiés ou falsifiés. Ces techniques relèvent d'un domaine que l'on appelle le « contrôle d'intégrité ».

De même, les outils de cryptographie et les certificats électroniques permettent d'assurer la confidentialité des données, ou l'authenticité des signatures électroniques. Le problème étant que ces méthodes, coûteuses en temps d'organisation et de contrôle, sont quasiment inappliquées par les entreprises, et encore moins par les particuliers.

Pour la messagerie électronique, les opérateurs ont renforcé la sécurité de leurs systèmes, et ces derniers enregistrent par ailleurs tous les courriers qu'ils sont amenés à traiter. Mais, aussi longtemps qu'il n'y aura pas de coordination internationale aux fins de faire évoluer les moyens informatiques sous-jacents à la messagerie électronique, et en vue d'en assurer la fiabilité juridique, il ne faudra pas attendre d'évolution majeure dans ce domaine.

Pour les services téléphoniques, notons simplement que le citoyen lambda ne peut rien faire pour améliorer la sécurité de ses échanges. Depuis le milieu des années 80, les technologies sous-jacentes à la téléphonie fixe et mobile n'ont quasiment pas changé : les opérateurs ajoutent de nouveaux protocoles d'échange (WAP, MMS, 3G+…) mais ne modernisent pas les anciens. Il ne s'agit ni plus ni moins que d'un château de cartes technologique élaboré sur des bases poreuses.

L'Etat, également, est très réticent à fournir aux particuliers des outils leur permettant d'assurer l'authenticité et la confidentialité de leurs échanges téléphoniques : on se doutera du pourquoi.

Pour finir, nous rappellerons que quasiment toutes les sécurités mises en œuvre pour la protection des écrits, et consacrées par le droit, s'appuient sur des systèmes de cryptographie.

Il sera amusant, pour le lecteur, de savoir que la sécurité induite par la cryptographie n'est pas « réelle » : elle existe du fait de notre incompétence à factoriser, en mathématiques, les multiples de très grands nombres premiers. Toute la sécurité des données, dans le monde, repose donc sur de l'ignorance.

L'avènement d'un ordinateur du futur (processeur quantique), ou de corpus mathématiques novateurs, peuvent, à terme, briser l'intégralité des sécurités cryptographiques existantes, y compris, bien sûr, celles consacrées par notre droit positif comme la signature électronique.

Conclusion

Le législateur doit-il aménager un nouveau régime juridique pour la gestion de la preuve électronique ? La définition abstraite de la preuve écrite électronique est-elle finalement trop souple ?

On ne saurait trop remettre en cause la définition de la preuve écrite électronique sans remettre en cause, de manière plus générale, la liberté de la preuve. Et ce, d'autant plus, que la preuve écrite électronique représentera, dans un avenir proche, un nombre croissant de preuves présentées devant les tribunaux.

Pour endiguer le risque de manipulations mal intentionnées, et de falsification des preuves, il importe tout d'abord que les acteurs de la justice, aussi bien les juges que les auxiliaires de justice, soient conscients des risques que les preuves électroniques engendrent. Cette conscience du risque ne peut se faire que par une éducation spécialisée sur ces nouvelles problématiques.

Par ailleurs, il faut également attendre des acteurs de l'informatique, industriels et ingénieurs, la mise en œuvre de nouveaux moyens, plus fiables, de communication et de réalisation des preuves.

La question de la sécurité juridique des actes numériques est aujourd'hui très peu prise en compte par les ingénieurs, lors de l'élaboration de nouveaux services ou protocoles de communication. Il importe que les acteurs de l'informatique soient conscients des risques juridiques qui découlent de la mise en œuvre de leurs outils de communication, ou de production. On ne peut plus se satisfaire de documents signés, sans notre accord, par des logiciels d'édition quelconques…

De manière générale, il semble donc qu'un meilleur niveau d'éducation permettrait de dégager des synergies juridiques et technologiques positives, visant à affermir la sécurité juridique des citoyens dans l'ère du tout numérique.

Cela passe notamment par la mise en place de formations spécialisées à destination des professionnels de l'informatique et du droit, mais également par l'information et la sensibilisation à long terme.