LEXBASE
l'information juridique

Revues

Lexbase Hebdo édition affaires n°280 du 18 janvier 2012

[Internet] Evénement

La preuve informatique — Quelles nouveautés techniques pour quelles évolutions juridiques ?

N° Lexbase: N9704BS9

ADIJ

par *Marylou Garcias et Max Chouzier, Membres de la "Section jeunes" de l'ADIJ*

Le 8 décembre 2011 avait lieu un colloque sur la preuve informatique, organisé par l'Association pour le développement de l'informatique juridique (ADIJ) en partenariat avec l'Agence nationale de la Recherche (ANR). De nombreux professionnels étaient réunis pour présenter les problématiques actuelles et les récentes évolutions, dans divers domaines juridiques, de la preuve informatique, thème pluridisciplinaire. Le débat était animé par Mme Isabelle de Lamberterie, Directrice de recherche émérite (CNRS-CECOJI) et ancienne présidente de l'ADIJ.

Il convient de brièvement exposer les règles relatives à la preuve informatique.

La preuve des actes juridiques revêt une importance capitale car le succès d'une action dépend de la manifestation de la légitimité de ses prétentions. Afin de mettre en place un cadre juridique sûr, il a fallu s'assurer de la prise en compte de la preuve informatique par les juges, et de son opposabilité à l'égard de tout contractant. En effet, dans les années 1990, en raison de l'utilisation accrue de l'informatique, déterminer la valeur de l'écrit électronique par rapport à l'écrit papier s'est avéré indispensable : quel document prévalait juridiquement sur l'autre ? Comment faire valoir juridiquement l'écrit électronique ? La loi du 13 mars 2000, portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique (loi n° 2000-230 N° Lexbase : L0274AIY), est ainsi intervenue sur cette question en modifiant les articles 1316 (N° Lexbase : L1427ABH) et suivants du Code civil.

La loi du 13 mars 2000 a opéré une petite révolution puisqu'elle a conféré à l'écrit électronique, en conformité avec les objectifs communautaires, la qualité de preuve légale, c'est-à-dire de mode de preuve parfait. En l'occurrence, elle a modifié l'article 1316 du Code civil, base légale de la preuve littérale, de façon à libérer cette preuve de tout support. L'article 1316-1 du Code civil (N° Lexbase : L0627ANK) va même plus loin puisqu'il consacre la forme probante de l'écrit électronique, sa recevabilité étant soumise à deux conditions : la personne dont il émane doit pouvoir être dûment identifiée et il doit être établi et conservé dans des conditions de nature à en garantir l'intégrité. Désormais, un document électronique a une valeur en dehors même des contrats et l'on peut, par exemple en matière de procédure, se prévaloir d'un acte accompli électroniquement à la place d'un écrit sur support papier, sauf lorsque cette forme est exigée. Le législateur reconnaît ainsi par l'article 1316-3 (N° Lexbase : L0629ANM) du même code que "*l'écrit sur support électronique a la même force probante que l'écrit sur support papier*".

En cas d'incertitude s'agissant de l'intégrité ou de l'authenticité entre deux preuves inscrites sur deux supports différents (papier et électronique), le législateur confie au juge la tâche de désigner la preuve la plus convaincante aux faits de l'espèce (C. civ., art. 1316-2 N° Lexbase : L0628ANL). De la sorte, le législateur refuse d'instaurer une différence entre la preuve électronique et la preuve traditionnelle. En pratique toutefois, un expert peut être commis pour décider du caractère probant dudit document.

La reconnaissance juridique de la signature électronique en droit français a permis une telle évolution. La signature, élément essentiel de la validité d´un écrit, est au sens traditionnel un lien unissant, par la voie de l'écrit, le corps du signataire avec l'écrit qu'il signe : elle établit et donne force au lien entre le signataire et le document signé. Ce faisant, la signature a la double fonction d'identifier le contractant, et de matérialiser son consentement. Or, l'exigence d'une signature manuscrite était inconciliable avec l'échange de messages électroniques. Il fallait reconnaître une valeur à la signature électronique. Si celle-ci a d'abord été consacrée par la Directive européenne sur la signature électronique du 13 décembre 1999 (Directive (CE) 1999/93 N° Lexbase : L0093AWD), il était nécessaire de recourir à un système fiable d'identification qui garantisse l'existence d'un lien avec l'acte auquel la signature se rattache.

La loi du 13 mars 2000 ne se contentera pas de veiller à la garantie du lien entre l'écrit et la personne, mais proposera une nouvelle finalité à la signature : garantir juridiquement l'intégrité du document, tant lors de sa conclusion que lors de son existence. Le problème se posait à l'aune du progrès électronique, la numérisation des documents permettant une reproduction parfaite de ceux-ci de sorte que personne ne pouvait distinguer l'original de la copie, sauf à ce que soient mis en œuvre les procédés recommandés par le législateur.

C'est ainsi que le décret du 30 mars 2001, pris pour l'application de l'article 1316-4 du Code civil et relatif à la signature électronique (décret n° 2001-272 N° Lexbase : L1813ASX), est venu préciser les conditions de mise en place de la présomption de fiabilité du procédé garantissant le lien entre l'auteur et l'acte. L'article 1316-4 du Code civil reconnaît ainsi ce lien entre l'acte et la signature : il doit être sans équivoque et à cette fin, la signature doit être indissociable du texte auquel elle se rattache. Ce lien participe donc de la sécurité des transactions. Le deuxième alinéa de ce texte établit également que la signature électronique sécurisée permet d'obtenir une présomption simple de fiabilité, mais nécessite un certificat électronique qualifié suivant le décret de 2001.

En outre, le décret institue une nouvelle catégorie de prestataires : les prestataires de service de certification électronique. Sont également créés les certificats électroniques, moyen technique unique permettant l'utilisation efficace d'une signature électronique. Ces procédés permettent au signataire, au moyen d'une clé privée qui lui est délivrée par le tiers certificateur, d'établir un lien entre l'acte qu'il réalise et cette clé. La personne qui prendra connaissance de l'acte pourra s'assurer, en interrogeant la clé publique du signataire détenue par la société de certification, que ce dernier n'a pas révoqué son certificat.

– **Présentation du projet LISE (*Liability Issues in software Engineering*)**

Les premiers intervenants ont été les responsables du projet LISE. Le colloque a ainsi débuté par la présentation de la "*Problématique générale du projet LISE soutenu par l'Agence Nationale de la Recherche*", par **Daniel Le Métayer, Directeur de recherche (INRIA Grenoble Rhône-Alpes)** et **Christophe Alleaume, Professeur de droit à l'Université de Caen Basse-Normandie**. Le projet LISE est une coopération fructueuse entre des spécialistes de la technique et du droit dans la mesure où les responsables du projet ont établi une jonction entre le droit et la technique. En effet, le projet LISE vise à anticiper les éléments de preuve pour faciliter le traitement des griefs au moyen d'outils techniques et juridiques. Plus précisément, il s'agit de fournir un ensemble de méthodes et d'outils, aussi bien informatiques que juridiques, pour permettre aux parties d'un contrat informatique, de définir précisément leur responsabilité en cas de dysfonctionnement de logiciel, de préciser les éléments de preuve et enfin, d'établir cette responsabilité. Le projet s'intéresse donc à la correspondance entre dysfonctionnements et responsabilité. Il établit des critères formels qui, une fois exploités, permettront de déterminer une responsabilité.

Le projet s'appuie sur la formalisation d'une architecture de logs, c'est-à-dire l'association entre des types d'événements (envois et réceptions de messages), des acteurs en charge d'enregistrer ces logs, et ceux en charge de les signer. La notion de log prône donc une démarche volontaire : l'individu souhaite extraire certaines "traces". A titre d'exemple, le type d'architecture acceptable serait de définir que tout événement qui pourrait avoir une influence sur le traitement d'un grief doit être enregistré quelque part. Il s'appuie également sur la formalisation de la notion d'acceptabilité. Prenons l'exemple d'un accord informel entre les parties : si le client affirme que le document qui lui a été présenté pour une transaction donnée était différent du document qui lui est opposé par le marchand et que son grief est valide, le fournisseur de l'application de signature sera alors responsable. Ce projet formalise donc les outils techniques existant en amont pour mettre en œuvre cette démarche d'anticipation.

Ensuite, **Nicolas Craipeau, Docteur en droit, Universités de Salamanque et de Nantes**, a présenté "*Les modes de preuve informatique prévus et non prévus par contrat*", dans la perspective de fixer un cadre juridique pour le

projet LISE. Quels étaient donc les modes de preuve informatique qui pouvaient être utilisés ? Il a fallu procéder à une première démarche de prospection ; faire un état des lieux et comprendre l'importance des conventions de preuve, du rôle du juge dans l'appréciation des preuves fournies (C. civ., art. 1316-2), et de la collecte de preuves par l'archivage électronique, qui doit garantir la conservation des "traces" probantes intègres selon des procédures sécurisées et élaborées sur la base de la norme l'AFNOR NF Z 42-013 relative à l'archivage électronique. Quant aux preuves légales, elles comprennent la signature électronique (C. civ., art. 1316-1 et 1316-3) et la signature électronique sécurisée. En somme des réglementations difficiles à mettre en œuvre.

Ainsi, il est apparu nécessaire d'adopter une démarche de création. Le droit positif en la matière étant plutôt abscons et difficile à mettre en œuvre, les responsables du projet ont opté pour la création d'une convention de preuve. Des preuves prévues par les parties permettraient la prise en compte des spécificités de l'informatique et de la complexité des systèmes concernés, la sécurisation des relations juridiques ainsi qu'une preuve rapide, fiable, et surtout à un coût réduit (notamment éviter la bataille d'experts pour le juge). Dès lors, quel était le cadre juridique des conventions de preuve en matière informatique ? Le principe est la liberté de la preuve dans les contrats B2B (C. civ., art. 1134 et 1316-2). Avant même l'intervention du législateur, la jurisprudence a utilement reconnu la validité des conventions relatives à la preuve : les règles de preuve ne sont pas d'ordre public (Cass. civ. 1, 8 novembre 1989, n° 86-16.197 N° Lexbase : A2014AH3 ; TGI Paris, 2 septembre 1997). Ces conventions ont ensuite été reconnues légalement par la loi du 13 mars 2000.

A la suite de cette application, Nicolas Craipeau a proposé une clause type selon laquelle les parties s'engagent à se soumettre aux règles de preuve définies par la convention, règles enregistrées, conservées de manière spécifique, et où l'on définit une durée de conservation en fonction des règles législatives.

– **La preuve numérique dans la procédure judiciaire : contraintes, validités, évolutions**

"*La preuve numérique : quel coût pour quel enjeu ?*" Telle est la question posée par **Serge Migayron, Expert près la Cour en Technologies de l'Information et Président de la CNEJITA**. Ce dernier a commencé par analyser la preuve numérique comme une démonstration qui associe un ou plusieurs éléments de nature numérique et un raisonnement. L'étape précédant la preuve est l'information numérique, ou *Electronically Stored Information* (ESI). Celle-ci est abstraite et complexe, puisqu'elle est portée par des architectures logiques complexes (réseau internet), ainsi que fragile, car facilement modifiable (un volume de l'Encyclopaedia Universalis est copiable en une minute sur une clé USB). Elle est également très riche quantitativement (on estime à 100 milliards le nombre de courriels échangés quotidiennement dans le monde). Pour être éligible au statut de preuve numérique, l'information numérique doit satisfaire certains critères stricts avant de pouvoir faire l'objet d'une interprétation technique qui précédera sa qualification juridique. Elle doit remplir les critères d'authenticité (origine de l'information), d'intégrité (contenu de l'information) et de traçabilité (chaîne de traitement de l'information).

En outre, le risque pesant sur la preuve numérique demeure l'effet du temps : en prévention d'une disparition ou d'une érosion de la preuve, il conviendra de procéder à des copies physiques ou à une reconstitution d'un environnement informatique. Serge Migayron propose donc l'invention de nouveaux moyens de preuve, du fait d'évolutions légales ou jurisprudentielles (systèmes d'archivage de messageries), ou du fait d'évolutions technologiques (Google, Amazon, Gmail, Google docs...).

Enfin, la question s'est posée de savoir comment maîtriser les coûts de la preuve numérique. Cette maîtrise peut se faire par le choix des mesures (cibler les postes, les serveurs, les volumes et les sauvegardes) et par l'anticipation des mesures (conservation des sauvegardes, constitution d'une documentation), qui tend à instaurer une culture de l'anticipation des preuves. Il faut retenir que les moyens de recherche de la preuve informatique doivent être proportionnés aux enjeux (preuve simple, preuve complexe, faisceau de preuves), et qu'il existe un juste prix pour chaque preuve informatique.

Ensuite, la problématique du *no-bridge* a été soulevée par **Paul Vidonne, Expert près la Cour, Directeur du LERTI et Maître de conférences à l'Université de Grenoble** : "*Preuve juridique et preuve scientifique : 'un cas de* no-bridge*'?*". Son questionnement est le suivant : la vérité scientifique peut-elle fonder la vérité judiciaire ? Voudrait-on faire prendre à l'expert tant la place du juge que celle de l'enquêteur ? A titre d'exemple, quand le juge demande un extrait du disque dur externe, son rôle de qualification de la preuve est transféré à l'expert. **Serge Braudo, Conseiller honoraire à la cour d'appel de Versailles**, définit la preuve comme "*la démonstration de la réalité d'un fait, d'un état, d'une circonstance ou d'une obligation*". La démonstration est celle apportée par des moyens de preuve soit parfaits (preuve légale) soit imparfaits (preuve libre). Cette définition laisse à penser que la science peut contribuer à démontrer la réalité d'un fait. Mais est-ce bien le cas ?

Il ajoute que la "vérité judiciaire" est constituée une fois la preuve admise, lorsque le fait, l'état, l'obligation, deviennent certains : "l*e droit n'a pas pour objet de comprendre le monde, mais de le faire fonctionner*". Quant à la "vérité

scientifique", elle consiste en la démonstration d'une vérité relative au monde réel, démonstration reposant sur une méthode scientifique reconnue (expérimentation, modélisation, raisonnement logique...). En effet, "*la science n'a pas pour objet de faire fonctionner le monde, mais de le comprendre*".

Selon Paul Vidonne, la notion de preuve numérique au sens scientifique répond à la question suivante : "*Comment un fait du monde réel peut-il être établi à partir d'informations partielles relatives à ce fait -et disponibles sous forme de données numériques— ?*". La collecte d'informations repose en effet sur des méthodes d'investigation, pour lesquelles existent une accréditation COFRAC des laboratoires (référentiel ISO 17 025) et une norme de AFNOR X 50-110 dite Prescriptions générales de compétences et d'aptitudes requises pour élaborer une expertise. Si celles-ci ne sont pas obligatoires, le respect de leurs orientations générales est une obligation morale (mise en place et respect de protocoles d'investigation, utilisation de moyens logiciels et matériels reconnus "*Forensic*", ...). Il souligne que la preuve numérique est la probabilité qu'un fait du monde réel soit vrai ; dès lors, comment distinguer le vrai du faux ? André Compte-Sponville, lors du XVIIème congrès national des experts judiciaires de Marseille du 22 octobre 2004, a estimé que "*la mission-type de l'expert est de dire le vrai, autant qu'on peut le connaître, c'est-à-dire le possiblement vrai et le certainement faux*". En outre, il est rappelé qu'il existe des probabilités fortes et des probabilités faibles. Les preuves établies par plusieurs moyens, telles qu'une date provenant de plusieurs sources différentes, ou encore les preuves recoupées par des tiers ou les preuves non discutées, ont ainsi une forte probabilité.

Paul Vidonne conclut par l'existence d'un *no-bridge* entre le droit et la science, la vérité juridique et la vérité scientifique appartenant à des mondes différents et hétérogènes. Il n'y aurait pas de "pont" entre des univers certains et probabilistes ; entre celui de la science et celui du droit. L'office du juge est alors "*d'accepter ou de refuser de transformer une probabilité scientifique et technique en un fait juridique, générateur de droits*". En l'occurrence, Jacques Hureau considère que l'expert, débiteur du vrai, est sollicité par le juge, débiteur du juste. Il termine par une pensée illustrative d'Aristote selon laquelle "*L'ignorant affirme, le savant doute, le sage réfléchit*".

– **Authentification, conservation et tiers de confiance : regards juridiques**

Thierry Piette-Coudol, avocat au barreau de Paris et président de l'association IALTA France, a ensuite présenté le cas particulier de "*L'authentification et la signature électronique : l'infrastructure créée par l'Ordre des Experts-comptables"*. La présentation portait sur la signature électronique dédiée à la profession d'expert-comptable : Signexpert, lancée en raison de la volonté des experts-comptables de se doter d'un système de signature électronique qui soit à la marque de l'Ordre. L'optique de Signexpert est avant tout de garantir une grande authentification et confidentialité des informations ; en somme, de signer et de sécuriser par exemple les documents pour les clients, les courriels, l'archivage électronique sécurisé. En conclusion, il estime que malgré son entrée dans le code napoléon depuis dix ans, la signature électronique est un outil encore trop peu utilisé et toujours en construction, probablement en raison de la défiance du monde du droit à l'égard du monde de la technique.

Puis, **Eric A. Caprioli, avocat au barreau de Paris et Vice-président de la Fédération nationale des Tiers de confiance**, a présenté "*Les tiers de confiance*". "*Comment conserver des données informatisées tenant lieu de documents à valeur juridique, lesquels restent soumis à des règles formulées le plus souvent pour l'archivage sur des supports papier ?*". L'intervention des tiers de confiance est une solution. Le rôle de ces tiers est de fournir la sécurité et la confiance dans les communications numériques en assurant des fonctions juridiques fondamentales telles que l'identification de l'auteur, l'intégrité et la non répudiation des messages. Les tiers de confiance contribuent en effet efficacement à l'établissement et à la conservation des preuves électroniques, et leur régime juridique est varié : il se compose de quelques dispositions législatives, de dispositions contractuelles, et s'appuie sur des normes techniques et des "bonnes pratiques".

Le recours à un tiers de confiance peut s'expliquer, les preuves établies en interne étant toujours acceptables devant un tribunal si elles sont considérées comme fiables. De plus, la responsabilité du tiers de confiance peut être engagée dans le cadre de ses services et obligations liés à la preuve électronique, et les coûts relatifs à la mise en œuvre des services de confiance sont moindres.

La notion de tiers de confiance est, en réalité, un terme générique désignant l'ensemble des fonctions pouvant être exercées par les tiers prestataires de services à valeur ajoutée dans les échanges électroniques. Dans le commerce électronique, il faut distinguer plusieurs catégories de tiers de confiance évoqués dans le décret du 30 mars 2001 et l'ordonnance du 8 décembre 2005 (ordonnance n° 2005-1516, relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives N° Lexbase : L4696HDB) : les prestataires de services de certification électronique (PSCE), les prestataires de services d'horodatage électronique (PSHE) et les prestataires de services de confiance. L'autorité de certification est une "*autorité chargée par un ou plusieurs utilisateurs de créer et d'attribuer leur clé publique et leur certificat*" (IUT-T Recommandation X 509). Identification/authentification/intégrité (signature électronique) ; horodatage ; chiffrement (éventuel) ; archivage. Telle est

la chaîne de confiance pour un écrit électronique.

Par la suite, **Jérôme Legrain, huissier de justice** et **Claude Bodeau, expert près de la cour et responsable de l'atelier ADIJ "évaluation du préjudice"**, évoquent la problématique de la preuve informatique sous l'angle du duo huissier-expert. Le métier de l'huissier est d'établir et rapporter la preuve, par un constat exclusif de tout avis. Il sera régulièrement accompagné d'un expert, sans lequel ses compétences se trouvent trop régulièrement dépassées par l'état de la technique et dont le rôle est de fournir des éléments plus comparatifs, des éléments de jugement. C'est ici l'occasion de signaler d'entrée qu'en matière de preuve électronique, on a pour l'essentiel transposé ce qui existait déjà en droit. Ainsi se pose l'exemple du domicile dans lequel l'huissier ne peut pas entrer sans l'autorisation de la personne ou de l'entreprise, ou sans une décision de justice. Il en va de même en matière électronique, le professionnel devant se cantonner, en l'absence d'autorisation, aux limites d'un univers qui reste accessible au public. Très tôt, par exemple, il a été jugé qu'un site web n'est pas un domicile (TGI Paris, 14 août 1996 ; TGI Paris, 5 mai 1997 ; TGI Paris, 10 juin 1997). Autre exemple, la question de la force probante du constat d'huissier ne change pas en matière de preuve électronique, mais il faut noter que cette question n'est pas figée. Une loi du 22 décembre 2010 (loi n° 2010-1609, relative à l'exécution des décisions de justice, aux conditions d'exercice de certaines professions réglementées et aux experts judiciaires N° Lexbase : L9762INU) est venue renforcer la force probante des constats puisqu'ils font, depuis, foi jusqu'à preuve contraire quand ils n'étaient jusqu'alors que de simples renseignements.

Il a fallu également s'adapter à de nouveaux supports, pour lesquels se posent de nombreuses réflexions juridiques et techniques et qui imposent donc à l'huissier d'être plus méticuleux que jamais dans l'établissement de la preuve. Le SMS est très tôt reconnu comme un moyen de preuve (Cass. civ. 1, 17 juin 2009, n° 07-21.796, FS-P+B+R+I N° Lexbase : A1897EI4), malgré la facilité déconcertante pour tout un chacun de falsifier ce type de communication. La collecte de preuve sur les réseaux sociaux est elle aussi parfaitement envisageable, dès lors que l'on demeure dans la sphère publique du réseau. On trouve ainsi un bel exemple de transposition du droit aux nouveaux usages de communication avec la possibilité pour un huissier d'opérer un constat avec l'assistance d'un "ami Facebook" qui dispose d'un identifiant et d'un mot de passe lui permettant de voir les informations litigieuses, comme il peut opérer un constat dans un immeuble si un voisin le lui permet, ou dans une foire ou un salon si l'un des exposants lui transfère un accès.

Toutes ces évolutions nécessaires, somme toute récentes, conduisent à un véritable problème juridique. La jurisprudence est confrontée à un monde mal maîtrisé et mal connu, ce qui occasionne une certaine insécurité juridique. Un exemple marquant est celui de la pratique des huissiers qui consistait à acheter des objets sur internet pour constater l'infraction de contrefaçon. Lorsque la troisième chambre de la Cour de cassation décida, à la surprise générale, qu'une telle pratique n'était conforme au droit, tous les constats se sont brusquement retrouvés annulés alors même que tous les professionnels estimaient agir dans le cadre de leurs prérogatives (réf ?). Un autre exemple tout aussi parlant est celui de la rédaction des ordonnances. L'huissier, dès qu'il est confronté à un obstacle, recourt à l'article 145 du Code de procédure civile (N° Lexbase : L1497H49) pour que le juge lève cet obstacle. Attention dès lors aux ordonnances mal rédigées, comme celle qui permettrait à l'huissier d'aller chercher des données sur l'ordinateur personnel d'un particulier sans penser à la possibilité qu'avait celui-ci de ne sauvegarder ses données que sur un support amovible, qui n'appartient pas à l'ordinateur personnel. Or, comme le rappelle Claude Bodeau, en conclusion, lorsque l'huissier cherche à effectuer un constat sur des données auxquelles il n'a pas accès, il respecte "*l'ordonnance, toute l'ordonnance, rien que l'ordonnance*".

La recherche de la preuve sur des supports informatiques amène tout naturellement à évoquer ensuite la question de la validité de la preuve dans le monde du travail. **Christine Baudoin, avocat au barreau de Paris, associée Lmt avocats et responsable de l'atelier ADIJ "droit du travail et nouvelles technologies"**, aborde le sujet en rappelant en introduction que, si la surveillance des salariés relève du pouvoir de direction et de contrôle de l'employeur, les juridictions ont largement insisté concomitamment, sur les droits et libertés fondamentaux des salariés, comme le souligne l'arrêt "Nikon" du 2 octobre 2001 (Cass. soc., 2 octobre 2001, n° 99-42.942 N° Lexbase : A1200AWD). Le principe, pour ce qui concerne les données hébergées sur le lieu de travail du salarié, est celui d'une présomption du caractère professionnel des données, et ce depuis un arrêt du 18 octobre 2006 (Cass. soc., 18 octobre 2006, n° 04-48.025, F-P+B N° Lexbase : A9621DRR). Il convient donc, dès lors que l'on estime que les données sont personnelles, de choisir un nom de fichier ou de dossier sans ambiguïté, afin de renverser la présomption. Le groupe de travail insiste d'ailleurs sur la pertinence d'aller au-delà de la mention "personnel", terme polysémique qui peut tout aussi bien recouvrir les ressources humaines (le personnel) que des données privées, pour lui préférer par exemple le terme de "privé". La preuve, donc, est irrecevable s'il est avéré que le dossier concerné ne relevait pas des documents de travail du salarié. Elle est recevable si l'on considère l'hypothèse de risques ou événements particuliers, dont l'identification, difficile, sera réglée au cas par cas.

Tout cela, toutefois, ne relève que d'un premier degré, celui qui consiste à savoir si l'on peut, ou non, ouvrir un

dossier, un document ou une communication du salarié. Il existe un second degré, trop souvent négligé, le fait d'avoir pu légalement ouvrir un document n'entraînant pas ensuite la possibilité d'utiliser devant le juge ce que l'on y a trouvé. On peut ainsi évoquer l'exemple de cette enveloppe Kraft, sans mention qu'il s'agissait d'un pli privé pour le salarié, et à l'intérieur de laquelle se trouvait une revue échangiste, pornographique. S'il a été reconnu que l'employeur était en droit d'ouvrir l'enveloppe, il lui a été refusé de l'utiliser ensuite contre le salarié (Cass. mixte, 18 mai 2007, n° 05-40.803, P+B+R+I N° Lexbase : A3179DWN).

Une fois encore, l'appréciation de la validité de la preuve se fera au cas par cas, avec toujours cette présomption de caractère professionnel des documents, qui s'applique aussi bien aux e-mails qu'à la simple connexion à internet depuis le poste de travail. Le simple fait, par exemple, d'avoir sur son navigateur une liste de favoris ne confère pas un caractère personnel à cette liste. Pour ce qui est des réseaux sociaux, enfin, la jurisprudence est très peu fournie, voire inexistante. On peut se reporter à l'arrêt de la cour d'appel de Reims en date du 9 juin 2010 (CA Reims, ch. sociale, 9 juin 2010, n° 09/3205 N° Lexbase : A2056E9Z), qui illustre bien cette dualité privée/publique du réseau Facebook. Notons enfin qu'à ce sujet, la CNIL a mis un place un document d'information sur son site internet pour aider à mesurer les conséquences de nos traces sur de tels réseaux.

Enfin, il convient de rappeler que ce n'est pas parce que la preuve est déloyale qu'elle ne peut être invoquée devant les juridictions pénales. Devant les juridictions sociales, elle doit être loyale mais aussi garantir son intégrité, critère important. Le salarié, de son coté doit aussi faire preuve d'une certaine loyauté, qui consiste en ne pas essayer de dissimuler la preuve. C'est l'hypothèse du salarié licencié non pas parce qu'il consultait des sites à caractère pornographique sur son temps de travail, mais parce qu'il effaçait de son navigateur les historiques correspondants (CA Rennes, 19 avril 2007, n° 06/03 156 N° Lexbase : A7035HCK).

.