



Preuve informatique Valeur juridique du document numérique

La loi du 13 mars 2000 reconnaît une valeur probante à l'écrit numérique. De nombreuses questions restent en suspens, notamment quant à la traduction des conditions posées par la loi en spécifications techniques ou aux moyens d'assurer l'efficacité de ces systèmes en cas de litige.

La valeur juridique du document numérique est un sujet d'actualité. Les colloques se multiplient. Magistrats, experts, avocats et opérationnels s'interrogent. Avec raison, car il y a un monde entre la vision technicienne et le ressenti des acteurs du droit.

Certes la loi a changé. Certes elle reconnaît la valeur probante de l'écrit numérique, à certaines conditions. Comment traduire ces conditions en spécifications techniques, comment assurer l'efficacité de ces systèmes complexes en cas de litige, ce sont les différentes questions que nous aborderons au travers d'un panel de sujets représentatifs des interrogations les plus fréquentes en la matière.

LA NOTION DE « PREUVE PAR ÉCRIT »

À l'aube de l'année 2000, la notion de « preuve par écrit » résultait d'une évolution bicentenaire, timidement accueillie par le Code civil en fonction des avancées de la jurisprudence pour reconnaître, comme mode de preuve légale, autre chose que le papier. Avec l'introduction massive de l'informatique et des réseaux dans la société civile et commerciale, il fallait une réforme. Ce fut chose faite avec la loi n°2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.

Aux termes de l'article 1316 du Code civil : « La preuve littérale, ou preuve par écrit, résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que

soient leurs supports et leurs modalités de transmission ».

Désormais, la preuve n'est plus liée au support autrefois considéré comme seul valable : le papier. Support rassurant et oh combien commode, puisque le document papier permet d'un seul coup d'œil d'en appréhender l'origine et l'information signifiante. Il n'en est pas de même pour le document électronique. Ce dernier nécessite une transcription de la suite d'octets enregistrée sur le support électronique (disque, bande, etc.) afin de la rendre intelligible à l'homme. On le sent bien, c'est là que les difficultés commencent. Comment garantir que cette suite d'octets n'a pas été modifiée lors de manipulations indétectables du support informatique ? Comment savoir si au cours du temps, il sera toujours possible de l'interpréter ?

Cette toute nouvelle reconnaissance légale de la preuve numérique doit néanmoins être doublement nuancée. Elle signifie, *à contrario*, que ce n'est pas parce qu'une information est numérique qu'elle est dénuée de valeur probante. Mais la preuve est une notion relative. Le document est probant tant qu'il n'est pas remis en cause. S'il est remis en cause, il faudra faire la démonstration de sa fiabilité. Premier écueil dans la destinée de la preuve numérique, qui aura subi de nombreuses transformations tout au long de son cycle de vie depuis sa naissance jusqu'à sa restitution : transmission, transformation de format, stockage sur différents supports, risque d'accès non contrôlé.

Quelques actes sont restés réfractaires à la dématérialisation et doivent toujours être établis sur un support

papier. Aux termes de l'article 1108-2 du Code civil, il s'agit des actes sous seing privé relatifs au droit de la famille et des successions, et des actes sous seing privé relatifs à des sûretés personnelles ou réelles, de nature civile ou commerciale, sauf s'ils sont passés par une personne pour les besoins de sa profession.

LES CRITÈRES JURIDIQUES DE LA VALEUR PROBANTE

Ces critères figurent à l'article 1316-1 du Code civil, texte fondamental introduit par la loi du 13 mars 2000 : « 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 ».

Il s'infère de cet article que la qualité de la conservation de l'écrit électronique est une condition de la validité de la preuve, mais la loi ne traite pas des modalités d'archivage. Cela n'est pas une lacune : la loi doit être indépendante de la technologie. Les références techniques, évolutives par nature, seront à rechercher dans l'état de l'art et dans la norme.

La loi ne donne pas de définition de la notion d'« intégrité ». Le respect de cette exigence juridique repose sur la fiabilité du processus mis en œuvre pour gérer le cycle de vie du document. En particulier, toute modification de format constitue une brèche dans la garantie de l'intégrité au sens technique du terme (dès que l'on touche

un « bit » d'un fichier, l'intégrité technique est en effet perdue) et devra être assortie d'une description précise du processus utilisé afin de montrer que le contenu informationnel n'a pas été modifié.

Le critère d'identification se rapporte quant à lui à la notion d'imputabilité : un document n'est générateur de droits et d'obligations que si l'on sait qui est « responsable » de l'exécution de ces obligations, ou qui peut se prévaloir de ces droits. Ceci n'implique pas nécessairement que le document soit signé : la grande majorité des documents émis par une entreprise ou une administration n'est pas signée. Mais on sait les imputer à une personne morale car ils sont émis sur un support caractéristique de celle-ci : papier à en tête ou document commercial comprenant l'identification de la personne morale, logo ou marque.

Une application de l'article 1316-1 du Code civil a été faite pour la première fois par la Cour de cassation dans son arrêt rendu par la seconde chambre civile le 4 décembre 2008. Dans cette espèce, une Caisse primaire d'assurance maladie présentait comme « copie informatique » d'un courrier papier une impression d'un fichier électronique dont il n'avait pas été prouvé qu'il « avait bien été établi le 20 janvier 2003 et conservé dans des conditions interdisant à la Caisse de modifier le contenu de ce document ». La Cour de cassation a dès lors considéré que la valeur probante de cette copie informatique n'était pas établie, puisque le respect des conditions posées par l'article 1316-1 du Code civil n'était pas démontré.

Le principe de la démonstration qui devra être faite à un juge à l'occasion d'un litige sur la valeur probante d'un écrit numérique est ainsi posé : il faudra être capable de rapporter d'une part l'origine et d'autre part l'intégrité du document numérique litigieux. Le principe est fort simple. La démonstration sera plus complexe. Elle aura d'autant plus de chances d'aboutir que certaines précautions, que nous mentionnerons ci-après, auront été prises lors de la mise en œuvre du processus dématérialisé et du système d'archivage.

Dans l'arrêt précité, la Cour de cassation va même plus loin, en considérant qu'une copie informatique dont la fidélité, l'inaltérabilité et l'intégrité ne

peuvent pas être démontrées ne peut être admise par le juge judiciaire : « *l'admission par le juge judiciaire d'une prétendue copie informatique qui ne présente aucune garantie de fidélité, d'inaltérabilité et d'intégrité n'est pas conforme aux exigences du procès équitable ; de sorte qu'en admettant que la preuve de l'exécution de son obligation d'information par la CPAM de la Marne serait rapportée par la seule production d'un document informatique dont rien ne permettait de garantir qu'il n'avait pas été établi par la caisse pour les besoins du litige, la Cour d'appel a violé l'article 6-1 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales* ».

Cette affirmation est intéressante non pas tant pour l'ajout des notions de « fidélité » et d'« inaltérabilité », qui sont techniquement inhérentes au concept d'« intégrité », mais surtout car elle met en exergue le risque d'élaboration a posteriori d'un document numérique falsifié qui aurait été établi pour les besoins du litige. La Cour exprime l'importance de cette considération par deux fois dans le même arrêt, lorsqu'elle indique par ailleurs que : « *nul ne peut se constituer de preuve à soi-même ; de sorte qu'en se fondant uniquement sur un document édité par la CPAM de la Marne pour les besoins de la cause [...], la Caisse a violé de plus fort l'article 1315 du Code civil* ».

Il en résulte une indication importante : si une entreprise conserve en interne des documents numériques, il lui appartiendra de mettre en place un processus technique fiable qui permette d'en assurer l'intégrité. On voit poindre, en vue de futurs litiges, l'intérêt de faire appel à des tiers professionnels dans le processus de traitement, d'échange et de conservation des documents numériques : la fiabilité du processus reposera sur les garanties apportées par lesdits professionnels, ce qui devrait en faciliter la démonstration dès lors que ces derniers proposeront des services conformes à l'état de l'art et, le cas échéant, certifiés (voir le chapitre sur la valeur juridique de la norme et impact de la certification).

LA SIGNATURE ÉLECTRONIQUE

Avant la loi du 13 mars 2000, aucun

texte légal ne définissait la notion de signature. Il était couramment acquis, par la jurisprudence et la doctrine, que celle-ci matérialisait l'engagement que prenait le signataire de respecter les obligations à sa charge contenues dans l'acte signé.

La loi du 13 mars 2000 a formalisé cette définition dans l'article 1316-4 du Code Civil : « *La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte* ».

Reste à savoir comment transposer le concept dans le monde numérique. C'est ce qu'a réalisé la Loi du 13 mars 2000 avec la disposition suivante, portée à l'article 1316-4 du Code Civil : « *Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache* ». La signature électronique doit être réalisée à l'aide d'outils permettant d'identifier le signataire : simple reproduction d'une exigence fondamentale de la signature.

Quant au « lien », il exprime – de façon quelque peu sibylline – qu'il faut relier la signature avec l'acte numérique pour être certain que c'est à cet acte-là qu'a consenti le signataire. L'exigence n'est pas nouvelle. Elle se trouve naturellement remplie dans l'environnement matériel puisque la signature est apposée sur le papier et que l'ensemble [signature/document papier] est sensé constituer un tout indivisible et inaltérable.

La pratique actuelle, issue de la directive européenne 1999/93/CE sur la signature électronique, consiste à utiliser pour signer électroniquement des systèmes reposant sur les technologies cryptographiques à clés publiques (ou asymétriques, ou encore PKI), distribuées et garanties par des entités qui jouent un rôle de « tiers de confiance » dans le dispositif. Le tiers de confiance (« Prestataire de Service de Certification Electronique » ou « PSCE » dans les textes juridiques) attribue à une personne les moyens qui vont lui permettre d'apposer une signature électronique sur des enregistrements numériques. La personne signe le document au moyen d'une « clé privée » qu'elle est seule à détenir (par exemple logée sur une carte à puce) et le destinataire vérifie l'intégrité du document et l'identité du

signataire au moyen d'informations qui sont fournies et garanties par le tiers de confiance.

Il se trouve que la signature électronique remplit de façon parfaite les deux fonctions permettant d'accorder une valeur probante à un écrit numérique car l'enregistrement fait l'objet d'un calcul d'empreinte [donc son intégrité peut être vérifiée] et il a été crypté à l'aide d'un identifiant, la clé privée, qui est propre au signataire [ce qui procure au document une garantie d'origine]. La signature électronique permet donc d'assurer l'imputabilité d'un document électronique et l'intégrité de celui-ci.

Il faut toutefois prendre en compte plusieurs facteurs quant à l'utilisation de cette technologie. La fonction d'imputabilité n'est remplie par la signature électronique que si c'est l'émetteur originaire du document – c'est-à-dire soit une personne physique agissant pour son compte, soit un représentant de l'entreprise qui est juridiquement responsable dudit document –, qui signe celui-ci avec les outils de création de signature qui auront été mis à sa disposition par un PSCE l'ayant préalablement dûment identifié.

Dans la pratique, les choses se passent rarement de cette façon. Soit les documents sont signés de façon automatique par un serveur de l'entreprise : c'est la signature « personne morale », qui n'est pas reconnue formellement par les textes juridiques mais qui est admise par l'administration fiscale pour la signature électronique des factures. Soit les documents sont signés non pas par leur émetteur mais par un tiers qui intervient dans le processus (cas typique des conclusions de contrats sur plate-forme web) : dans ce cas, la signature ne remplit pas une fonction d'imputabilité mais constitue simplement un outil de sécurisation du cycle de vie du document.

La conservation d'un document électronique signé implique la mise en œuvre d'une application lourde afin de pouvoir revérifier la signature à tout moment pendant la durée de conservation du document. De plus en plus, la pratique tend à prendre en compte cette contrainte en intégrant dans les processus un indicateur de validité de la signature au moment de la transaction (délivré par un tiers ou par le PSCE) et conservé ensuite en métadonnée par le système d'archivage.

LA DATATION DE L'ENREGISTREMENT NUMÉRIQUE

La notion de date d'un écrit numérique n'est pas abordée dans les textes juridiques. Elle est néanmoins essentielle, car en cas de litige, la date constitue un élément déterminant de la valeur probante du document produit. Ce point est rappelé par la Cour de cassation dans son premier arrêt sur l'écrit numérique rendu par la seconde chambre civile le 4 décembre 2008. Dans cette espèce, une Caisse primaire d'assurance maladie présentait comme « copie informatique » d'un courrier papier une impression d'un fichier électronique dont il n'avait pas été prouvé qu'il « avait bien été établi le 20 janvier 2003 et conservé dans des conditions interdisant à la Caisse de modifier le contenu de ce document ».

L'importance de la date est également mentionnée dans le bulletin officiel des impôts n°4 du 11 janvier 2007 relatif à la possibilité pour les entreprises de garder uniquement un double électronique des factures papier émises (point 16) : « *L'opération d'enregistrement doit intervenir à une date la plus proche possible de celle de l'opération d'impression de l'original de la facture sur support papier. Le système informatique doit permettre d'identifier ces deux dates* ».

L'arrêt susvisé rappelle également le principe selon lequel on ne peut pas se constituer de preuve à soi-même. Appliqué à l'horodatage d'un document numérique produit par l'entreprise, cela signifie qu'il doit être de préférence assuré par des jetons d'horodatage fournis par un tiers, dont la fiabilité pourrait être apportée en cas de litige.

Enfin, lorsque la date d'expédition d'un document fait courir un délai légal, il est essentiel de conserver cette date par le biais d'un moyen technique fiable et pas uniquement la date de versement en archive, qui peut être différente. A ce jour, aucun texte réglementaire n'est venu préciser les conditions permettant de définir la fiabilité d'une méthode de datation d'un fichier informatique mais la pratique et les normes permettent de définir l'état de l'art en la matière.

VALEUR JURIDIQUE DE LA NORME ET IMPACT DE LA CERTIFICATION

Un écrit numérique a une valeur probante dès lors que l'on peut démontrer son origine et son intégrité depuis sa création (article 1316-1 du Code civil). En cas de contestation de cette valeur probante, la technicité du domaine est telle que les juges feront appel à des experts qui s'en remettront à des références extérieures pour déterminer la fiabilité des systèmes d'« archives à valeur probante » qu'ils auront à évaluer.

Ces références extérieures sont les normes et il est important de comprendre l'interaction de la norme et du droit aux fins d'en faire un juste usage dans le cadre de la conception d'un système d'archivage numérique.

En droit, les règles de l'art constituent le standard d'appréciation de la faute

La violation des règles de l'art est une expression couramment employée pour désigner tout manquement dans l'exercice d'une activité professionnelle. Les règles de l'art constituent par conséquent le standard à l'aune duquel s'apprécie la faute : est fautive l'exécution d'une prestation non conforme aux règles de l'art. En matière d'archivage numérique, cela signifie qu'un système qui serait conçu au mépris des règles de l'art serait vraisemblablement a priori considéré comme non fiable.

Distinction des règles de l'art et des normes techniques

Un courant majoritaire de la doctrine considère que la norme constitue une formalisation écrite des règles de l'art (Cf. notamment Lamy droit économique, partie 4, livre 2, division 2, chapitre 3, section 3). Sous une réserve toutefois, car par nature, les règles de l'art sont évolutives : le respect des règles de l'art implique du professionnel qu'il remette périodiquement son savoir en question. Ecrites, les normes techniques ne présentent pas un tel caractère. Alors que les règles de l'art ne sont jamais menacées d'obsolescence, les normes techniques peuvent l'être dès lors qu'elles ne représentent plus le dernier état de l'art raisonnablement accessible.

La norme est donc représentative de l'état de l'art, dès lors qu'elle est à jour. Le droit positif, dans le sillage d'un certain nombre d'arrêts rendus par la Cour de cassation, tend d'ailleurs à reconnaître aux normes une valeur forte d'indicateur de qualité d'un produit ou service.

En pratique, la documentation de conception et de suivi du système d'archivage devra préciser les aspects sur lesquels le système se conforme à telle ou telle norme. Dès lors que cette documentation d'archivage et les normes de référence seront régulièrement remises à jour, le respect de la norme constituera en cas de litige un élément important de l'appréciation de la fiabilité du système d'archivage par l'expert et le juge.

Impact de la certification

Une documentation bien conçue d'un système d'archivage doit donc faire référence à une ou plusieurs normes. Mais ceci reste du domaine de l'auto-déclaration. Dès lors qu'un organisme tiers vérifie la conformité d'un processus dématérialisé à une norme (ce qui suppose qu'il existe un référentiel de conformité pour cette norme), cette vérification confère une légitimité bien plus importante au processus certifié. Il s'agit de l'opération dite de « certification ».

L'opération de certification n'emporte une reconnaissance juridique exprès que si celle-ci est prévue par la loi. À titre d'exemple, c'est uniquement parce que la loi le prévoit que la signature électronique « sécurisée », soumise à un processus de certification par des organismes dont la désignation est prévue par les textes, présente une présomption de fiabilité. Et encore ne s'agit-il que d'une présomption qui, au titre de l'article 288-1 du Code de procédure civile, peut être écartée par le juge : « Lorsque la signature électronique bénéficie d'une présomption de fiabilité, il appartient au juge de dire si les éléments dont il dispose justifient le renversement de cette présomption ».

Il n'en reste pas moins que la certification présente l'avantage considérable de contribuer à créer un environnement de confiance. Il est aujourd'hui bien plus facile de falsifier un document papier qu'un document numérique créé et conservé dans les « règles de l'art ». Mais dans l'inconscient collectif, dans la pratique quoti-

dienne des juges, le papier reste la preuve royale. Il n'est que rarement remis en cause, contrairement à l'écrit numérique qui sera d'office contesté par celui à qui le doute profitera et dont la contestation risque, pour un moment encore, d'être favorablement accueillie par les magistrats. Certains, devant ce constat, baissent les bras et se demandent s'il ne vaut pas mieux conserver les bons vieux papiers. Et certes il le faut, dans certaines circonstances. Mais il y a de nombreux cas où le recours à l'échange et à la conservation numérique apporte un incontestable gain de qualité, de rapidité et de fiabilité. Là sans doute faut-il faire l'effort de la certification et/ou du recours à des professionnels certifiés et la confiance suivra.

ORIGINAL ET COPIE NUMÉRIQUE – PREMIÈRE APPLICATION JURISPRUDENTIELLE À UN PROCESSUS HYBRIDE

La notion d'« original » et la notion de « copie » dans le Code civil

Le Code civil comporte dix sept références au terme d'« original » mais aucune définition de cette notion. Cela n'est guère étonnant, tant elle paraît évidente, dans une civilisation où le seul support envisageable pour l'écrit est matériel. Le Petit Robert la définit comme un « ouvrage de la main de l'homme, dont il est fait des reproductions » ou encore « qui émane directement de l'auteur, est l'origine et la source première des reproductions ».

Les références à l'original apparaissant dans le Code civil se rangent dans trois catégories. La première est celle des actes « importants » : testaments, opposition au mariage ou à la reconnaissance de paternité, remise de dette, révocation du mandat.

L'original, écrit de la main même de celui qui pose ses dernières volontés, dégage un débiteur de sa dette, ou révoque la confiance donnée par écrit à un mandataire, revêt une valeur presque « sacrée », tant le poids physique et émotionnel de l'auteur transparaît dans les mots tracés de sa main sur un document « original ». C'est dans cette catégorie que se rangent d'ailleurs, en France, certains des actes qui ne peuvent toujours pas être dématérialisés.

La seconde concerne le droit de la preuve et le rapport hiérarchique établi par notre droit entre l'original et la copie. Nous avons reproduit ci-dessous certaines de ces dispositions car elles montrent bien la prééminence de l'original sur la copie dans notre système juridique traditionnel.

Article 1348 : « Les règles ci-dessus [...] reçoivent aussi exception lorsqu'une partie ou le dépositaire n'a pas conservé le titre original et présente une copie qu'en est la reproduction non seulement fidèle mais aussi durable. Est réputée durable toute reproduction indélébile de l'original qui entraîne une modification irréversible du support ».

Article 1334 : « Les copies, lorsque le titre original subsiste, ne font foi que de ce qui est contenu au titre, dont la représentation peut toujours être exigée »

La troisième concerne les originaux des contrats et comprend la seule disposition du Code civil relative à l'original qui ait été adaptée pour prendre en compte l'écrit numérique :

Article 1325 : L'actes sous seing privé qui contiennent des conventions synallagmatiques ne sont valables qu'autant qu'ils ont été faits en autant d'originaux qu'il y a de parties ayant un intérêt distinct.

Il suffit d'un original pour toutes les personnes ayant le même intérêt. Chaque original doit contenir la mention du nombre des originaux qui en ont été faits. Néanmoins, le défaut de mention que les originaux ont été faits doubles, triples, etc., ne peut être opposé par celui qui a exécuté de sa part la convention portée dans l'acte. L'exigence d'une pluralité d'originaux est réputée satisfaite pour les contrats sous forme électronique lorsque l'acte est établi et conservé conformément aux articles 1316-1 et 1316-4 et que le procédé permet à chaque partie de disposer d'un exemplaire ou d'y avoir accès.

La notion d'original est difficilement transposable dans le monde numérique, car son essence provient du lien physique qui s'établit entre l'auteur et l'acte, visible sur l'acte même auquel a consenti son auteur. Dans cette acceptation, l'original électronique n'existe pas. Ce qui s'en rapproche le plus est probablement l'écrit signé électroni-

quement. Le dernier alinéa de l'article 1325 du Code civil fait en effet référence à l'article 1316-4 du même code, qui définit la signature électronique.

Dans la pratique, les documents électroniques sont pratiquement tous des copies. La notion d'original est remplacée par la capacité du processus mis en œuvre à garantir l'intégrité du contenu informationnel depuis la création du document sous sa forme définitive et, par la suite, tout au long de son cycle de vie.

Particularité des processus hybrides

Tous les processus ne sont pas dématérialisés de bout en bout. Actuellement, de nombreuses applications de l'archivage numérique sont faites dans le cadre de processus dits « hybrides » : le document est créé sous forme électronique à l'aide des outils du système d'information, avant d'être imprimé sur papier. Cette impression, revêtue ou non de la signature manuscrite d'une personne de l'entreprise, est considérée comme un document original.

Autrefois, l'entreprise en faisait une copie papier qu'elle conservait dans un « chrono ». Cette pratique tend à disparaître avec la multiplication des documents, et le plus souvent seule une copie électronique est conservée au sein de l'entreprise, dans des conditions qui sont rarement conformes aux « règles de l'art » susvisées.

Cette évolution des pratiques fait apparaître une question nouvelle, qui est celle de la valeur juridique de la copie électronique en cas de conflit entre l'original papier et la copie, ou encore en cas de perte de l'original papier.

L'arrêt rendu le 4 décembre 2008 par la seconde chambre civile de la Cour de cassation s'est fondé sur l'article 1348 du Code civil pour apprécier la valeur probante d'une copie issue d'un processus hybride : « Alors, de quatrième part, que lorsqu'une partie n'a pas conservé l'original d'un document, la preuve de l'existence de ce document peut être rapportée par la présentation d'une copie qui doit en être la reproduction non seulement fidèle mais durable ; que la Cour d'appel a constaté que le document litigieux présenté par la Caisse, qui ne comportait pas la signature de son

auteur, comme la copie d'un courrier d'information prétendument envoyé par la CPAM de la Marne le 20 janvier 2003 avait été « édité sur un papier à en-tête revêtu d'un logo diffusé en 2004 » ; qu'en ne tirant pas les conséquences de cette constatation dont il résultait que le document n'était pas une copie fidèle du prétendu courrier d'information original, la Cour d'appel a violé les articles 1334 et 1348 du Code civil ».

L'originalité de cet arrêt est de rappeler un élément qui est parfois oublié lors de la conservation de copies électroniques de documents originaux papier : la copie doit être fidèle. Cela signifie qu'il ne suffit pas, comme l'avait fait la Caisse en l'espèce, de conserver le fichier du courrier dans un quelconque format de traitement de texte. Dans un processus hybride il faut conserver une reproduction électronique qui soit une image exacte du document papier original, comprenant notamment les mentions du papier à en tête et, si, le document papier était signé, la signature qui a été apposée sur l'original.

COMMENT VA SE DÉROULER UNE CONTESTATION PORTANT SUR UN ÉCRIT NUMÉRIQUE ?

Notre système juridique, au travers de dispositions contenues tant dans le Code civil que dans le Code de procédure civile, a laissé au juge un large pouvoir d'appréciation quant à la validité de la preuve, notamment numérique, qui lui est soumise.

Article 1316-2 Code civil : « Lorsque la loi n'a pas fixé d'autres principes, et à défaut de convention valable entre les parties, le juge règle les conflits de preuve littérale en déterminant par tous moyens le titre le plus vraisemblable, quel qu'en soit le support ».

Article 287 NCPC : « Si la dénégation ou le refus de connaissance porte sur un écrit ou une signature électroniques, le juge vérifie si les conditions, mises par les articles 1316-1 et 1316-4 du Code civil à la validité de l'écrit ou de la signature électronique sont satisfaites »

Le juge devra donc, en particulier, vérifier que le document a conservé son intégrité, ou qu'il est bien imputable à telle personne morale ou physique. Cette vérification passera par

une analyse complète du cycle de vie du document, qui sera d'autant plus complexe que le document est ancien et que son cycle de vie comprend des ruptures non maîtrisées.

La notion du cycle de vie complet du document est en effet encore largement méconnue par les entreprises qui envisagent de mettre en œuvre des processus d'archivage numérique. Il ne suffit pas de garantir l'intégrité du document à partir de son versement dans le système d'archivage mais il faut pouvoir aussi reconstituer ce qui s'est passé avant, et – plus précisément – ce qui s'est passé entre le moment où le document est dans son état définitif (l'« original ») et celui où il a été versé en archive.

Il faut ici mettre en garde contre deux excès. Le premier consistant à ignorer totalement la question et le second consistant à échafauder des implémentations d'une redoutable complexité technique, alors même que – par exemple s'il s'agit d'un contrat conclu à distance –, une partie du cycle de vie du document n'est pas sous contrôle.

Les litiges sur la preuve numérique appelleront des démonstrations techniques qui passeront par l'expertise. Aux fins de mettre toutes les chances de leur côté, les recommandations suivantes pourront être utilement suivies par les concepteurs des processus dématérialisés : raccourcir et simplifier le cycle de vie des documents ; le documenter de façon régulière en montrant la conformité à une ou plusieurs normes reconnues et à jour ; le faire auditer par un expert de façon régulière ; avoir recours à des tiers de confiance ; faire certifier le processus par rapport à la norme de référence choisie.

PRISE EN COMPTE DES DONNÉES PERSONNELLES

Les données personnelles font l'objet d'un encadrement juridique visant à établir un équilibre entre les nécessités des entreprises et les libertés individuelles : la Loi 78-17 du 6 janvier 1978 dite « Informatique et libertés », auxquelles s'ajoutent les décisions et recommandations de la Cnil (<http://www.cnil.fr>).

Un système d'archivage constitue un traitement de données personnelles

au sens de la Loi Informatique et libertés et il doit, à ce titre, faire l'objet d'une déclaration à la Cnil (le cas le plus courant étant celui des systèmes de messagerie).

La Cnil a émis le 11 octobre 2005 une délibération relative à l'archivage électronique dans les entreprises qui distingue les archives courantes, intermédiaires et définitives :- les archives courantes sont les données d'utilisation courante par les services concernés dans les entreprises, organismes ou établissements privés (par exemple les données concernant un client dans le cadre de l'exécution d'un contrat)- les archives intermédiaires sont les données qui présentent encore pour les services concernés un intérêt administratif, comme par exemple en cas de contentieux, et dont les durées de conservation sont fixées par les règles de prescription applicables.

- Les archives définitives sont exclusivement les données présentant un intérêt historique, scientifique ou statistique justifiant qu'elles ne fassent l'objet d'aucune destruction.

Les archives courantes et intermédiaires doivent répondre à des durées de conservation spécifiques, proportionnées à la finalité poursuivie (en particulier au regard des durées de prescription définies par la réglementation commerciale, civile ou fiscale), qui doivent être précisées dans le cadre des dossiers de formalités préalables adressés à la Cnil. Les responsables de traitement doivent établir dans le cadre de leurs moyens d'archivage, des procédures aptes à gérer des durées de conservation distinctes selon les catégories de données qu'ils collectent et soient en mesure d'effectuer, le cas échéant, toute purge ou destruction sélective de données à caractère personnel

La Cnil recommande que les archives définitives soient conservées sur un support indépendant, non accessible par les systèmes de production, n'autorisant qu'un accès distinct, ponctuel et précisément motivé auprès d'un service spécifique seul habilité à consulter ce type d'archives (par exemple la direction des archives de l'entreprise). La Cnil recommande également que les archives définitives « sensibles » soient anonymisées.

Enfin, et cela rejoint la nécessité de produire une documentation d'archivage, la Cnil recommande que les entreprises définissent, dans le cadre

de procédures formalisées, des règles d'archivage répondant à l'ensemble des préconisations précitées et qu'une information puisse être fournie sur ces règles, en cas de demande exprimée de leur part, aux individus faisant l'objet des traitements archivés.

CONCLUSION

La mise en œuvre d'un processus d'échange et de conservation de documents numériques est un projet à part entière. Il nécessite la coordination de plusieurs compétences au sein de l'entreprise, dont la compétence juridique. L'analyse juridique est structurante dans tout projet d'archivage car elle doit intervenir en amont pour dimensionner le projet selon ses trois axes fondamentaux.

L'axe de la valeur probante des documents conservés : dès lors que les documents en question revêtent un enjeu probatoire fort, les modalités de conservation doivent respecter les règles de l'art en la matière.

L'axe des obligations réglementaires, ou de conformité, qui s'appliquent à un type de données ou d'applications particulières, soit à raison du type de donnée concernée (donnée personnelle, donnée comptable, e-mail, etc.), soit à raison du secteur d'activité (secteur pharmaceutique, secteur bancaire, etc.).

L'axe de la durée de conservation, qui s'infère soit de textes spécifiques, soit de l'application des règles sur la prescription.

À ces trois axes il convient de rajouter une dimension supplémentaire, qui est celle de l'international. Pour la plupart des entreprises, le projet ne peut pas se cantonner à une vision franco-française car il va concerner différents pays.

Il est difficile d'établir des règles générales pour la conduite de tels projets, mais il existe cependant des constantes, qui sont les suivantes :

La conservation de documents numériques est un domaine très normé au plan international. Le respect des normes les plus reconnues dans chacun des pays couverts par le projet est indispensable.

Le raisonnement exposé plus haut, pour structurer le projet en amont, est

valable quel que soit le pays : pour dimensionner le système, il faut commencer par répondre aux questions suivantes : quel est l'enjeu probatoire, quel est l'enjeu réglementaire, quelle est la durée de conservation ?

L'administration de la preuve est différente d'un pays à l'autre car elle est liée à l'organisation judiciaire du pays, qui connaît des variations importantes selon le territoire considéré. La question devra nécessairement faire l'objet d'une analyse locale afin d'en saisir correctement l'enjeu.

Il n'y a pas de solution unique pour l'archivage de tous les documents de l'entreprise. Tout projet de conservation de documents numériques doit commencer par une opération de qualification. Selon la typologie des documents considérés, on déterminera l'enjeu associé à la qualité de leur valeur probante, aux éventuelles règles de conformité auxquelles ils sont soumis, à leur durée de conservation et ce, pour chacun des pays couverts par le projet d'archivage. L'enjeu associé à certains documents ne justifie pas la mise en œuvre de processus lourds et complexes car le risque afférent peut être cantonné et provisionné (certains contrats conclus en ligne avec les consommateurs par exemple). Pour d'autres documents, par exemple les factures transmises par voie électronique, l'enjeu financier est tel qu'il n'est pas envisageable d'ignorer les préconisations de l'administration fiscale en la matière. Deux documents, deux preuves, deux mesures...

Isabelle Renard
*Avocat associée,
Docteur ingénieur
Racine, cabinet d'avocats*