ARCHIVAGE A VALEUR PROBATOIRE

Définition

L'archivage dit « à valeur probatoire » consiste à mettre en œuvre un ensemble de procédés permettant de conserver durablement des données numériques et d'en garantir l'authenticité, l'intégrité la pérennité et la traçabilité, de leur prise en charge jusqu'à leur restitution, transfert ou destruction.

La durée de conservation peut varier de quelques mois à plusieurs dizaines d'années selon la nature de l'archive (factures, relevés de banque, dossiers médicaux, etc…). Certaines archives, dites « patrimoniales », sont conservées sans limitation de durée.

La terminologie « valeur probatoire » est utilisée pour signifier que les données archivées sont recevables d'un point de vue légal, à condition que puisse être démontré de manière certaine, fiable, dès leur prise en charge par le système d'archivage et à quelque moment que ce soit :

- qu'elles sont bien ce qu'elles sont réputées être (authenticité)
- qu'elles n'ont été ni modifiées ni altérées, volontairement ou non (intégrité)
- qu'elles peuvent toujours être restituées de manière intelligible (pérennité)
- que toutes les preuves liées aux actions réalisées peuvent être produites (traçabilité)

Les procédés mis en œuvre comprennent de nombreuses techniques matérielles et/ou logicielles (authentification, journalisation, cryptographie, signature électronique, …).

Exemples

D'innombrables applications de l'archivage à valeur probatoire sont possibles : archivage de bulletins de paye des salariés, de contrats et de factures, , de messages électroniques, de fichiers audio, de logs d'audit de sécurité des systèmes, de transactions bancaires, de dossiers médicaux, etc.

Illustrons notre propos avec l'archivage des bulletins de paye et des factures…

L'archivage des bulletins de paye des salariés par un employeur nécessite que ce dernier les conserve pendant 5 ans. Le salarié, lui, doit respecter cette obligation à vie. Lorsque l'envoi de ces documents se fait de manière dématérialisée, employeur et salarié doivent utiliser des dispositifs leur permettant de se conformer aux législations en vigueur, incluant de fait le caractère « à valeur probatoire » de l'archivage.

Pour les factures (B2B), chaque partie doit les conserver pendant 10 ans à compter de leur émission. Les factures papier numérisées doivent toujours être conservées. En revanche, si une facture électronique est imprimée pour être transmise, la conservation du double papier n'est pas obligatoire pourvu que le dispositif permette de « garantir l'authenticité, l'intégrité et la pérennité du contenu électronique depuis l'émission de l'original papier jusqu'à l'expiration de la période de stockage informatique. » (cf. Instruction Fiscale du 11 Janvier 2007)

Cibles

Le marché ciblé par l'archivage à valeur probatoire est aussi vaste que son champ d'application. En théorie, tout le monde (ou presque) peut être concerné, du professionnel (contrats, factures, actes, …) au particulier, et ce afin de respecter les législations en vigueur.

Ainsi et par exemple, en France, des durées de conservation précises sont définies pour divers types de documents, que ce soit pour des sphères privées ou publiques, professionnelles ou particulières. Avec l'essor de la dématérialisation (au sens « tout numérique » du terme), il devient donc impératif de disposer d'outils permettant un archivage à plus ou moins long terme et offrant une valeur juridique certaine aux documents conservés pendant toute la durée de celle-ci.

L'opposabilité des documents (ou plus généralement des informations) archivés permet par exemple à une banque de garantir ses transactions, à une assurance ses contrats, aux impôts les déclarations de revenus, …

Cadre réglementaire

Le cadre réglementaire (d'un point de vue électronique) est fixé en France principalement par trois textes :

- 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
- loi n°2004-575 du 21 Juin 2004 pour la confiance dans l'économie numérique (LCEN)
- articles 1316-1 et 1316-4 du Code Civil sur les conditions impératives que doit revêtir un échange électronique pour acquérir une force probatoire
- norme AFNOR NF Z42-013 de Mars 2009 portant sur les spécifications relatives à la conception et à *l'exploitation de systèmes informatiques en vue d'assurer la conservation et l'intégrité des documents* stockés dans ces systèmes

Il est aussi nécessaire de prendre en compte différents textes n'étant pas relatifs à des écrits purement électroniques, mais néanmoins applicables, qu'il s'agisse de normes, lois, décrets, voire jurisprudence.

Il existe également un certain nombre de réglementations sectorielles, fixant là encore des exigences sur des domaines d'activités précis (santé, administration, finance, etc), avec parfois des compléments ou des ajustements liés au caractère dématérialisé des opérations. En voici deux exemples :

- Sarbanes-Oxley (ou SOX) : loi fédérale US sur la réforme de la comptabilité des sociétés cotées et la protection des investisseurs. C'est un passage obligé pour le monde de la finance internationale,
- CFR 21 Part 11 : édicté par la FDA (Food & Drug Administration), cette réglementation spécifie la façon dont doivent être gérés les informations numériques et les signatures électroniques. Là encore, malgré son caractère américain, elle est couramment requise dans le milieu de la santé.

Dans un cadre plus large (Européen ou International), citons les textes clés suivants pour ce qui concerne les aspects électroniques des informations :

- ISO 15489 (Information and Documentation – Records Management) – Norme internationale fixant les exigences de gestion des enregistrements électroniques
- MoReq2 (Model Requirements for the Management of Electronic Records) du DLM Forum – Exigences pour la maîtrise de l'archivage électronique (actuellement en révision)
- DoD5015.2 (Electronic Records Management Software Application Design Criteria Standard) du Département de la Défense US – Exigences pour la gestion des enregistrements électroniques

Evaluation des risques

Les risques encourus si l'on ne met pas en place une solution d'archivage à valeur probatoire sont principalement juridiques et, par voie de conséquence, financiers car l'impossibilité de présenter en cas de litige une preuve irréfutable devant un tribunal peut entrainer une condamnation. Généralement, il s'agit d'amendes, dont le montant peut atteindre des sommes très importantes, mais, potentiellement, le risque peut être encore plus grave (disparition de l'entreprise si son image s'en retrouve entachée, peines de prison ferme ou avec sursis, …).

Avec la progression croissante des échanges sous forme numérique, la question de leur valeur juridique se pose donc comme un élément essentiel de cette analyse, car il devient inévitable de se demander comment une information peut être opposée à un tiers et quelles sont les conséquences si cela s'avère impossible.

Une des premières jurisprudences française sur le sujet concerne un litige opposant la société Continent France (Groupe Carrefour) à la CPAM de la Marne au sujet de la prise en charge d'un accident du travail. La CPAM doit informer l'employeur de la reconnaissance ou non du caractère professionnel de la maladie ou de l'accident. La CPAM prétendait avoir envoyé le 20 Janvier 2003 un courrier simple à Continent, ce dernier déclarant ne l'avoir jamais reçu. La copie du courrier envoyé par la CPAM avait été « édité sur un papier à en tête revêtu d'un logo diffusé en 2004 » ; il en résultait que le document n'était pas une copie fidèle du prétendu courrier d'information original. La Cour de Cassation a donc rejeté la validité de ce fichier bureautique simple, jugeant que cet écrit électronique ne valait pas preuve car l'auteur n'était pas dûment identifié et qu'il n'avait pas été « conservé dans des conditions de nature à en garantir l'intégrité ».

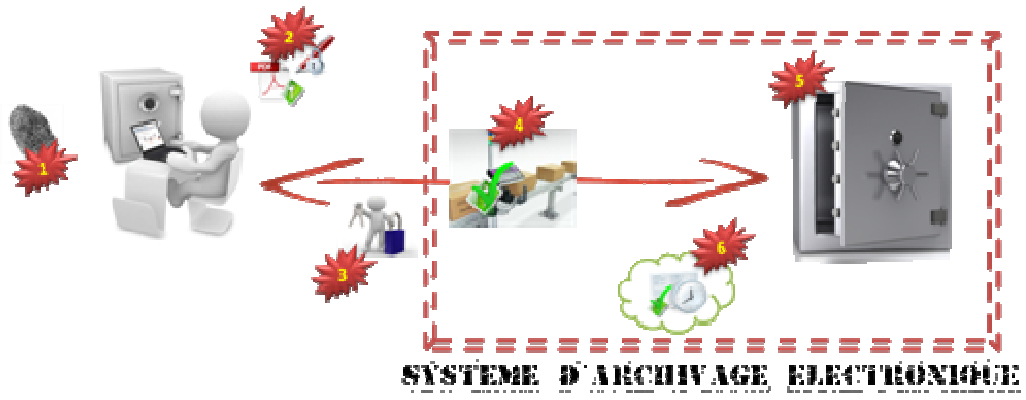
Un autre exemple plus récent, dans un arrêt du 2 Juillet 2010 relatif à une affaire entre deux sociétés spécialisées dans la fabrication et la distribution de bijoux et le site M6-Boutique, une des preuves a été rejetée par la Cour de Cassation au motif que l'outil du site sur lequel étaient archivés les documents était dépourvu de force probante. De plus, il n'était pas démontré que les différentes opérations d'affichage, de modification, de retrait et d'archivage correspondaient à la date mentionnée dans la référence de ce cheminement (*source legalis.net*). Bien que le montant du dédommagement ne soit pas très élevé (5000 €), ceci apporte un autre éclairage sur les risques encourus.

A contrario, dans une affaire opposant EBay à quatre sociétés de parfums, un constat APP (Agence pour la Protection des Programmes) conforme à ces exigences de valeur probatoire a été jugé recevable. Les sociétés de parfum reprochaient à EBay d'avoir laissé des entreprises commercialiser leurs produits sans autorisation sur son site. Les constats APP le prouvaient. EBay a ainsi été condamné, au vu des preuves, à verser un total de 706 000 € aux quatre sociétés de parfums.

Ces quelques exemples montrent que l'analyse des risques doit attacher une attention toute particulière aux problématiques liées à la confiance dans les systèmes de conservation et d'échange de données, notamment lorsque celles-ci peuvent être utilisées dans le cadre de procédures judiciaires.

Moyens de protection

Nous disposons d'une large gamme de procédés que nous avons schématisés ci-après :



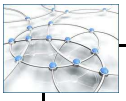
Nous considèrerons qu'il y a fondamentalement deux « acteurs » dans les cinématiques, l'utilisateur et le Système d'Archivage Electronique (SAE). En définitive, le SAE sera le « garant » de la valeur probatoire des données qui lui sont confiées, et formera ainsi une première sphère de confiance numérique grâce à six mécanismes de protection :

1. authentification et/ou identification des utilisateurs dans le système
2. calcul d'empreintes et signature électronique des données
3. sécurisation des échanges avec le SAE
4. contrôle de validité des données entrantes
5. stockage des données dans un coffre fort numérique
6. journalisation de toutes les actions réalisées par le système

Voici les caractéristiques les plus notables de ces rideaux défensifs :

- l'authentification, qui peut faire intervenir des procédés de chiffrement, de biométrie, de cartes à puce, rendant certaine l'identité de l'acteur réalisant une opération sur une archive
- le calcul d'empreintes numériques, basé sur des algorithmes cryptographiques complexes, permettant d'obtenir un condensat unique et infalsifiable des données
- la signature électronique, associant à des données une empreinte réalisée à une date certaine (horodatage via une autorité tierce) et par une personne clairement identifiée (utilisation de certificats électroniques valides et non révoqués, délivrés par une autorité de confiance)
- le chiffrement des données échangées, généralement par le biais de clés dites asymétriques (ou à clés publiques / clés privées)
- le contrôle des données, notamment par la vérification des empreintes, des certificats électroniques utilisés pour la signature par rapport à des politiques d'archivage, de signature, …
- l'implantation d'un coffre fort numérique, assurant le calcul d'empreintes internes, la gestion des supports de stockage physique, la durée de conservation, l'autocontrôle régulier de son intégrité, …
- la traçabilité complète des évènements, enregistrés séquentiellement dans des journaux rendus inaltérables par un horodatage, un chaînage (empreinte du journal précédent incluse en en-tête du journal courant) et déposés au moins une fois par jour dans un coffre-fort numérique (interne ou tiers)

A cela, il faudrait également rajouter la pérennisation, dans la mesure où il convient de procéder sur le long terme au « rafraichissement » des empreintes numériques avec des algorithmes plus résistants ainsi que des formats de données assurant leur lisibilité permanente.



Liens utiles

Pour plus d'informations, se référer à la documentation disponible sur le sujet, et notamment les sites Internet suivants :

- JOURNAL OFFICIEL : http://www.journal-officiel.gouv.fr/
- AFNOR : http://www.afnor.org/
- ISO : http://www.iso.org/iso/fr/home.htm
- FEDISA : http://www.fedisa.eu/
- FNTC : http://www.fntc.org/