

« Conservation et archivage de l'écrit sous forme électronique »

Thierry Piette-Coudol, avocat du barreau de Paris

in Jurisclasseur Communication et commerce électronique – mai-juin, cf 12 et 14

Résumé par Marie-Anne Chabin pour la réunion du PIN du 15 janvier

L'article constate tout d'abord que la période de deux ans depuis la promulgation de la loi 2000-230 du 13 mars 2000 ayant fait de l'écrit électronique une preuve potentielle au même titre que l'écrit papier (article 1316 du Code civil) est trop courte pour tirer des conclusions mais que le problème de la conservation est posé par la loi qui mentionne le fait que l'écrit électronique doit être conservé, sans toutefois dire comment.

L'auteur remarque que les juristes privilégient le terme de *conservation* et les techniciens celui d'*archivage*, les deux mots étant souvent employés l'un pour l'autre, la conservation étant plutôt le « résultat final à atteindre » et l'archivage un procédé dynamique pour l'atteindre.

La première partie est intitulée : « La conservation et la préparation de l'archivage »

La loi du 13 mars 2000 définit la signature électronique comme un « procédé fiable d'identification » et l'auteur en tire la notion d'un « procédé fiable de conservation ». En s'appuyant sur divers textes (rapport « Internet et les réseaux numériques » du Conseil d'Etat (1998), loi Madelin de 1994 sur le commerce électronique, norme ISO 15489 sur le Records management, la norme 42-013 sur l'archivage électronique, etc.), l'auteur analyse et compare la notion de fiabilité avec plusieurs notions qui s'y rattachent : la durabilité (du support), l'irréversibilité, la fidélité, la pérennité.

Il distingue la lisibilité et l'intelligibilité de l'écrit électronique (document crypté lisible non intelligible), présentées comme des garanties secondaires de l'écrit électronique. Quant aux garanties principales, priorité est donnée à l'intégrité sur l'identification. L'identification ne peut être assurée que par un tiers certificateur qui vérifie la signature. L'intégrité doit être constante, à chaque phase du cycle de vie du document. Sur la notion d'intégrité, le droit français étant peu disert, l'auteur s'appuie sur la loi québécoise n° 161 relative au cadre juridique des technologies de l'information (juin 2001) qui énonce les qualités de stabilité, pérennité et intégralité demandées à l'écrit électronique (nuance entre intégrité et intégralité). Toutefois, la loi québécoise ne décrit pas précisément quel procédé garantit cette intégrité.

La traçabilité apparaît comme une garantie complémentaire qui n'est pas demandée par le droit mais qui se révèle plus concrète dans la mesure où lui correspondent un certain nombre d'actions identifiées. Les normes NF 42-013 et ISO 15489 notamment, mais aussi l'article 289 bis du Code général des Impôts relatifs à la télétransmission des factures électroniques, évoquent une série d'actions propres à assurer la traçabilité : historisation (listes récapitulatives) des opérations et des événements, pistes d'audit, enregistrement systématique des métadonnées, enregistrement des opérations de certification, journalisation des événements pour le tiers certificateur (et archivage du journal), formalisation de toutes les procédures dans une charte d'archivage (ISO 15489).

La seconde partie est intitulée : « Une pratique de l'archivage conforme au droit »

L'auteur distingue 4 phases dans la pratique de l'archivage électronique à des fins de conservation :

1. la mise en archive : elle intervient forcément après la transaction et est le fait, soit de l'émetteur, soit du destinataire. Il convient de déterminer les éléments à archiver : l'écrit proprement dit, sa signature et, pour pouvoir valider la signature lors du désarchivage, le certificat électronique (lequel change tous les deux ans...), et donc la clé publique contenue dans ce certificat (la clé privée ne peut être légalement conservée que par son propriétaire).
2. l'éventuelle intervention d'un tiers archiveur : l'article renvoie au *Guide de l'archivage sécurisé* publié en juillet 2000 par un groupe de travail composé de juristes et d'experts-comptables. Le lot d'éléments à archiver, s'il est envoyé à un archiveur externe, fait lui-même l'objet d'une signature électronique pour sécuriser la transmission. L'enjeu est l'intégrité de l'écrit, avant et après le ou les changements de support. La loi québécoise n° 161 est très claire sur ce point. Les données techniques ou « données de service » adjointes au document sont tracées en tant que telles et ne remettent pas en cause son intégrité.
3. le stockage à proprement parler : puisque le but de l'archivage est la possibilité de le consulter, la localisation de l'archive doit être connue. Il faut distinguer la localisation géographique (voir la directive 2001/115 et le stockage des factures électronique dans un autre Etat) et la localisation technique (disque Worm dans NF 42-013). Le stockage doit être tracé, ainsi que la destruction de l'archive.
4. le désarchivage : ce terme désigne la restitution, c'est-à-dire le déstockage et l'expédition au demandeur avec les mêmes méthodes de sécurisation, notamment une signature électronique de l'envoi (*Guide de l'archivage sécurisé*). La notion de fidélité de l'écrit restitué (sous forme papier ou électronique), par rapport à l'écrit électronique d'origine revient, adossée à la notion d'intégrité et à la traçabilité des opérations garantissant l'intégrité. En cas de désarchivage en interne, le certificat d'horodatage peut servir à cette vérification.

En conclusion, l'auteur constate les lacunes de la loi française sur cette question de l'intégrité, heureusement compensée par les normes techniques. « Le législateur devra formuler l'exigence d'un procédé fiable garantissant l'intégrité ».