La Gazette des archives

Risque juridique et dématérialisation

Antoine Meissonnier

Risque juridique et dématérialisation

Antoine MEISSONNIER

Introduction : le risque du « risque zéro »

D'après le *Trésor de la langue française*, le risque est la « possibilité hasardeuse d'encourir un mal, avec l'espoir d'obtenir un bien »[1]. La dématérialisation se place dans cette optique : les acteurs qui la mettent en œuvre espèrent un bien (gain de temps, d'espace, d'exploitabilité, donc d'argent) moyennant quelques risques (forte variabilité des données numériques accroissant les risques de falsification et de perte de données, obsolescence technique). Les archivistes savent bien combien ces risques sont sous-estimés par les décideurs et combien la dématérialisation jouit d'un présupposé positif sur ses bienfaits.

Une partie des risques liés à la dématérialisation est pourtant bien prise en compte par les spécialistes de la sécurité des systèmes d'information *via* plusieurs méthodes d'analyses des risques[2]. Plus audibles que les archivistes dans les administrations, ces experts peuvent également rencontrer des difficultés à faire prendre en compte leurs préconisations à mesure que l'informatique se démocratise[3]. Autre versant du risque induit par la dématérialisation, le risque

[1] Article « Risque », dans le *Trésor de la langue française* : http://atilf.atilf.fr/.

[2] La lutte contre les risques informatiques est précisément le sujet de la série de normes ISO 27 000 et suivantes. On peut aussi citer des déclinaisons de ces dernières : la méthode d'*Expression des Besoins et Identification des Objectifs de Sécurité* (EBIOS) de l'Agence de la sécurité des systèmes d'information (ANSSI) ou encore la *MÉthode Harmonisée d'Analyse des RIsques* (MEHARI) mise au point par le Club de la sécurité de l'information français (CLUSIF).

[3] Les actualités font pourtant régulièrement état de failles de sécurité entraînant la divulgation de données confidentielles ou à caractère personnel. Voir par exemple l'étude menée dernièrement par trois étudiants du *Center for IT-Security, Privacy and Accountability* de l'université de la Sarre (Allemagne) : *via* un moteur de recherche spécialisé, ils ont pu avoir accès à des milliers de bases de données MongoDB contenant notamment des données à caractère personnel (HEYENS (Jens), GRESHAKE (Kai), PETRYKA (Eric), *MongoDB databases at risk: Several thousand MongoDBs without access control*, Université de la Sarre, CISPA, janvier 2015 : http://cispa.saarland/wp-content/uploads/2015/02/MongoDB_documentation.pdf).

juridique devrait être plutôt l'apanage des juristes. Mais rares sont les juristes spécialistes de ce domaine qui mêle des connaissances de tous les types de droits. En outre, de par mon expérience, les juristes ne sont pas, contrairement aux informaticiens, familiers de l'analyse des risques et établissent souvent une réponse fondée sur la recherche du risque zéro.

Pourtant, comme le montre le sociologue Christian Morel, la recherche du risque zéro est elle-même un risque. Il établit une distinction entre deux manières d'appréhender la lutte contre les risques dans des domaines soumis à des risques importants, comme l'aviation, la marine nucléaire ou encore le ski hors-piste : d'une part, l'usage de la rationalité substantielle et, d'autre part, celui de la rationalité procédurale[1].

La première se fonde sur une volonté d'atteindre le risque zéro en quantifiant chaque facteur de risques pour arriver à distinguer les situations qui sont en substance dangereuses de celles qui ne le sont pas. Christian Morel prend ainsi l'exemple de l'appréhension du risque d'avalanche par les adeptes du ski hors-piste : pour évaluer ce risque, on a d'abord cherché à mettre au point un test par prélèvement permettant de déterminer si le manteau neigeux était propice à une avalanche. Mais comment savoir si ce prélèvement est représentatif du manteau neigeux ? Ce dernier présente en général une grande variabilité sur une même pente. Suite à plusieurs accidents survenus en Suisse dans les années 1980, une autre méthode, typique de la rationalité procédurale, a été élaborée : elle a pris pour objectif, non de déterminer dans quelle situation précise le risque n'existait pas, mais de faire chuter la probabilité d'accidents mortels. Pour ce faire ont été déterminées des procédures qui limitent le risque : renoncer aux pentes d'une certaine orientation et inclinaison suivant le niveau global de risque d'avalanche évalué par les institutions météorologiques, tenir compte de la présence de traces fraîches, espacer les skieurs, etc. Grâce à cette approche, une diminution nette des accidents mortels a été observée en Suisse, ce qui n'a pas été le cas en France, où la première méthode reste privilégiée[2].

À la lumière de cet exemple, on conçoit le danger de se focaliser sur la recherche du risque zéro : dans le cas du ski hors-piste, il est impossible de rassembler toutes les informations qui seraient nécessaires pour déterminer sûrement les situations exemptes de risques. Viser le risque zéro entraîne alors la personne qui doit prendre la décision dans un processus cognitif assez

[1] MOREL (Christian), *Les décisions absurdes II*, Paris, Gallimard, coll. « Folio Essais », 2012, p. 78-83.
[2] *Ibid.*, p. 132-135.

aléatoire. Dans le cas de la dématérialisation, on n'a effectivement pas toujours accès à la bonne information, mais surtout les risques encourus ne sont pas d'une gravité extrême (aucun mort n'est encore à déplorer à ma connaissance…). De ce fait, comme on l'a dit, les décideurs ont en général un *a priori* favorable à la dématérialisation compte-tenu de ses bienfaits : si l'archiviste use de rationalité substantielle pour tenter d'écarter tout risque et aboutit à l'idée qu'il conviendrait mieux de renoncer à un projet de dématérialisation, il court le risque d'être exclu du projet, qui se fera tout de même compte tenu de l'acceptabilité politique et sociale des risques pointés, et de ne pas pouvoir mettre en pratique ses méthodes de travail. Or, celles-ci pourraient bien être des procédures efficaces pour diminuer la probabilité du risque.

Dans le domaine de la dématérialisation, il n'est pas forcément nécessaire d'opposer systématiquement ces deux approches de lutte contre le risque. Les deux peuvent être associées, comme nous allons le voir. La rationalité procédurale me semble néanmoins un concept important à conserver à l'esprit pour exploiter au mieux ses compétences et ne pas se décourager face à l'impasse à laquelle peut parfois conduire une approche guidée par la rationalité substantielle. Elle a l'avantage en outre d'introduire pleinement la notion de probabilité, qui est en fait centrale dans la pratique professionnelle de l'analyse de risque : un *manager* du risque doit évaluer la gravité des risques et leur probabilité. C'est notamment le principe de la méthode MOSAR[1]. En fonction de ces deux paramètres, on pourra décider de l'acceptabilité du danger encouru et mettre ou non en œuvre des mesures préventives.

Cet article ne prétend pas faire le tour de l'ensemble des risques encourus lors d'un projet de dématérialisation. Il va se concentrer sur la question du risque juridique, c'est-à-dire essentiellement celui de perdre un procès mettant en cause la responsabilité du producteur des documents ou des données considérés. Il s'agira tout d'abord de donner les critères permettant d'identifier les situations les plus risquées à éviter, puis de décrire des cas moins clairs pour lesquels la meilleure méthode est encore de prévoir des procédures qui diminueront le risque juridique encouru.

[1] Méthode Organisée et Systémique d'Analyse de Risques.

Des documents à risque à identifier

Un projet de dématérialisation doit avant tout s'attacher à identifier, dans le processus qu'il transforme, les documents suivants :

▪ les actes juridiques, tels que définis en droit civil. Un acte juridique est en effet une manifestation intentionnelle qui traduit la volonté d'une personne de réaliser certains effets de droit (vente, legs, don, etc.) ;

▪ les décisions de l'administration, concept défini à l'article L200-1 du Code des relations entre le public et l'administration (CRPA).

Les actes juridiques

Dans le premier cas, les dispositions du Code civil prévoient assez précisément les règles de formalisation *ad probationem*[1] (art. 1316-1 et 4) et *ad validitatem*[2] (art. 1108-1) nécessaires pour qu'un acte juridique puisse exister sous forme électronique et être reçu comme preuve devant les tribunaux[3].

Le Code civil prévoit qu'un écrit électronique témoignant d'un acte juridique a une valeur probante sous les conditions suivantes :

▪ la personne dont il émane doit pouvoir être dûment identifiée (art. 1316-1) ;

▪ le document numérique doit être établi et conservé dans des conditions de nature à en garantir l'intégrité (art. 1316-1) ;

▪ étant nécessaire à la perfection de l'acte juridique en ce qu'elle permet l'identification des parties et traduit leur consentement, la signature se traduit

[1] Conditions de formalisation de l'écrit témoignant de l'acte juridique nécessaires pour que ce document soit recevable à titre de preuve devant les tribunaux.

[2] Conditions de formalisation de l'écrit témoignant de l'acte juridique nécessaires pour que l'acte juridique soit valide. Ce type de conditions n'existe pas forcément pour tous les actes, mais, lorsque c'est le cas, ces conditions l'emportent sur les conditions de formalisation *ad probationem*. En effet, si les conditions *ad validitatem* ne sont pas remplies, l'acte est réputé n'avoir jamais existé. Il ne pourra logiquement pas être produit à titre de preuve devant les tribunaux.

[3] L'ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations va modifier la numérotation de ces articles du Code civil à partir du 1er octobre 2016. Ils deviendront respectivement les articles 1366, 1367 et 1174.

dans le domaine électronique par l'usage « d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache » (art. 1316-4). C'est ainsi que le décret d'application du 31 mars 2001 définit la signature électronique. L'article 1316-4 prévoit en plus l'existence d'un procédé d'identification « dont la fiabilité est présumée jusqu'à preuve contraire » qui implique donc un renversement de la charge de la preuve[1] : c'est le procédé décrit dans le décret du 31 mars 2001, qui est appelé « signature électronique sécurisée ». Ce dernier dispositif n'est cependant pas une condition nécessaire à la perfection de l'acte juridique, mais un niveau supplémentaire de sécurité juridique.

Les critères de formalisation *ad validitatem* sont les mêmes puisque l'article 1108-1 du Code civil se borne à renvoyer aux articles 1316-1 et suivants[2].

Les décisions de l'administration

Les décisions de l'administration relèvent du droit administratif et donc pas du Code civil. Le droit de la preuve y est libre. Néanmoins, des préconisations existent sur leurs conditions de validité.

Ainsi, l'article L212-1 du CRPA prévoit bien que « toute décision prise par une administration comporte la signature de son auteur ainsi que la mention, en caractères lisibles, du prénom, du nom et de la qualité de celui-ci »[3].

Au-delà des décisions des autorités administratives, d'autres documents produits par l'administration peuvent faire l'objet de conditions de formalisation qui viennent limiter fortement les possibilités de dématérialisation. On peut ranger ces conditions en deux grands ensembles :

---

[1] Ce sera alors à la personne mettant en cause le document de prouver que le procédé de signature électronique n'est pas fiable.

[2] Ces principes de formalisation des actes juridiques connaissent néanmoins des exceptions. D'abord, en matière prud'homale, la preuve est libre (arrêt de la Cour de Cassation n° 98-44.666, Chambre sociale, 27 mars 2001). Notons en outre la plus importante dans notre vie quotidienne : tout acte mettant en jeu des sommes inférieures à 1500 € est dispensé de formalisation par écrit (art. 1 du décret n° 80-533 du 15 juillet 1980 pris pour l'application de l'article 1341 du Code civil). Dans ce cas, la preuve est libre : c'est sous cette exception que nos transactions commerciales sont possibles sans signature systématique de contrat.

[3] En tout état de cause, l'article L212-2 du CRPA exempte de cette obligation « les décisions administratives qui sont notifiées au public par l'intermédiaire d'un téléservice conforme à l'article L. 112-9 et aux articles 9 à 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 ». La difficulté est que la notion de téléservice n'est aujourd'hui pas définie précisément en droit.

▪ des dispositions relatives au support du document : par exemple, le Code général des collectivités territoriales oblige les communes à la tenue de leurs registres de délibérations, d'arrêtés et de décisions sur support papier (articles R2121-9, R2122-7 et R2122-7-1)[1] ;

▪ des mentions expresses de la nécessité d'une signature sur le document : c'est notamment le cas dans le Code de la santé publique, qui mentionne régulièrement des documents médicaux devant être signés par le personnel de santé ayant réalisé la prise en charge, ou l'ayant suscité, ou par le patient[2]. En cas de contentieux devant la justice impliquant des versions dématérialisées de ces documents, le juge s'appuiera sur l'article 1316-4 du Code civil : si le document a été signé manuscritement avant d'être dématérialisé, sans qu'une signature électronique ne vienne confirmer son authenticité, il y a un risque que le juge estime que les conditions de validité du document ne sont pas remplies et le rejette comme preuve.

Dans ce dernier cas comme pour les décisions des administrations, il n'est pas dit qu'en contexte électronique cette signature doive être une signature électronique conforme à l'état de l'art, mais le juge peut être amené à le penser[3].

En effet et tout d'abord, l'article L212-3 du CRPA indique que les administrations peuvent signer électroniquement leurs actes. Si elles le font, cette signature doit être conforme aux préconisations du Référentiel général de sécurité (RGS)[4].

En outre, même si le régime de la preuve est libre en droit administratif, on observe que le juge administratif a tendance à s'appuyer également sur les articles 1316-1 et suivants du Code civil que nous venons de voir pour étayer sa décision de recevoir un document électronique à titre de preuve. Il peut alors en venir à considérer que, si le document est électronique et devait être signé,

---

[1] Pour plus d'informations, voir l'annexe 1 du Vade-mecum du Service interministériel des Archives de France, *Autoriser la destruction de documents sur support papier après leur numérisation. Quels critères de décision ?* mars 2014 : http://www.archivesdefrance.culture.gouv.fr/static/7429.

[2] Code de la santé publique, L1131-1, R1112-3 et 58, R1131-19 et 20, R1211-19, R1232-3, R2132-11, R4127-76, R4311-8 et 14, R4312-29, R6211-21 et 44, D5134-9…

[3] Une administration a informé le Service interministériel des Archives de France d'un jugement de ce type concernant un système de gestion des ressources humaines dématérialisé. Les arrêtés de décision individuelle étaient produits sous forme numérique, sans signature électronique. Or le juge a rejeté l'arrêté produit par l'administration en s'appuyant sur l'article 4 de la loi du 12 avril 2000, devenu l'article L212-1 du CRPA.

[4] Voir : http://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/.

on ne peut lui présenter à titre de preuve qu'un document revêtu d'une signature électronique conforme à l'état de l'art. Un tel raisonnement empêche notamment toute production en justice d'un document numérisé revêtu uniquement de la signature manuscrite de son auteur[1].

Des règles à respecter impérativement

Si on envisage un projet de dématérialisation incluant des documents conformes aux cas que nous venons de voir, il est indispensable de se doter d'un système de signature électronique conforme à l'état de l'art[2], permettant d'identifier les auteurs des actes, et d'un dispositif de conservation adéquat des documents électroniques signés[3].

Dans ces cas, il faut également écarter tout projet visant à détruire des documents originaux signés après qu'ils ont fait l'objet d'une numérisation. La numérisation de la signature manuscrite n'étant en aucun cas une signature électronique conforme à l'état de l'art, le juge rejettera ces copies électroniques non signées électroniquement. Comme il n'est pas possible de refaire signer électroniquement par leurs auteurs les copies électroniques des documents papier, la dématérialisation de tels documents ne pourra se faire que sous la forme d'une production électronique native, suivie d'une validation par une signature électronique.

Certes, l'article 1348 du Code civil, communément cité dans le contexte de la dématérialisation, affirme qu'est recevable à titre de preuve, en cas de perte de l'acte original, « une copie qui en est la reproduction non seulement fidèle mais aussi durable. Est réputée durable toute reproduction indélébile de l'original

[1] Décision n° 351931 du Conseil d'État, 5e et 4e sous-sections réunies, 17 juillet 2013, § 5 : « [...] que, pour regarder comme constitutif d'une faute le fait que les comptes rendus d'analyse étaient revêtus d'une simple signature numérisée des biologistes qui les avaient établis, la chambre de discipline s'est fondée sur l'absence d'un procédé technique fiable garantissant l'authenticité de cette signature [...] » (les comptes rendus d'analyse de laboratoire doivent être signés conformément à l'article R6211-21 du Code de la santé publique).

[2] Même si le Référentiel général de sécurité n'est obligatoire que pour les administrations, on pourra toujours s'y référer utilement pour le choix d'une solution de signature électronique. Il faut néanmoins noter que le règlement (UE) n° 910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (dit règlement « eIDAS ») va imposer à partir du 1er juillet 2016 un référentiel commun de la signature électronique pour le secteur public comme privé.

[3] Suivant le besoin de pérennisation, ce pourra être une solution incluant un composant de coffre-fort électronique ou un système d'archivage électronique complet.

qui entraîne une modification irréversible du support ». Cet article ne concernait pourtant pas initialement l'électronique[1], le législateur s'étant refusé à ouvrir cette exception à la copie électronique, qui n'est pas réputée durable[2]. La normalisation a tenté de rendre cette exception compatible avec le numérique en définissant les critères d'une copie numérique fidèle et durable, notamment au travers de la norme NF Z 42-013 (WORM[3] physique, puis WORM logique), ce que la jurisprudence est venu reconnaître récemment[4]. Un nouvel article 1379 va remplacer l'article 1348 du Code civil : ses dispositions, applicables à partir du 1er octobre 2016, vont entériner cette approche.

Dans le reste des cas, des procédures à mettre en place pour limiter le risque

En dehors de ces cas, l'insécurité juridique règne. Dès lors que les documents apportent la preuve d'un fait juridique[5] ou seront utilisés dans les domaines du droit pénal, social ou administratif, le régime de la preuve est libre. Le juge va juger en son âme et conscience de la recevabilité des informations qui seront portées à sa connaissance comme preuves. Si aucune mention de formalisation *ad validitatem* ne vient attirer son attention, il y a de fortes chances de pouvoir apporter devant lui, sans risque excessif, la preuve du propos que l'on cherche à défendre avec des documents ou données numériques. Par conséquent, rien n'est impossible, mais ce qui est recevable par les juges n'est pas défini, sinon par une jurisprudence éparse et parfois contradictoire. Il sera vain d'essayer d'estimer le risque précis à dématérialiser tel ou tel document.

---

[1] Il était de fait, lors de sa rédaction, adapté à la reproduction sur microformes.

[2] SENAT, *Rapport sur le projet de loi portant adaptation du droit de la preuve aux technologies de l'information et relatif à la signature électronique*, Charles Jolibois (rapporteur), rapport n° 203, Commission des lois, 1999-2000 : http://www.senat.fr/rap/l99-203/l99-2035.html#toc32.

[3] *Write Once, Read Many* : se dit originellement des supports non réinscriptibles (WORM physique). On parle aujourd'hui de WORM logique pour désigner des systèmes d'information garantissant l'intégrité des données qui y sont conservées, grâce à un contrôle des modifications.

[4] Cour d'appel de Lyon, 3 septembre 2015, n° 13-09.407.

[5] Un fait juridique est un événement, volontaire ou non, susceptible de produire des effets juridiques, non du fait d'individus, mais du fait de dispositions légales. Deux jurisprudences récentes sont venues confirmer le principe de liberté de preuve d'un fait : l'arrêt n° 12-16.839 de la Cour de cassation, Chambre civile, 13 février 2014 et l'arrêt n° 11-25.884 de la Cour de cassation, Chambre sociale, 25 septembre 2013 : « attendu que les dispositions invoquées par le moyen ne sont pas applicables au courrier électronique produit pour faire la preuve d'un fait, dont l'existence peut être établie par tous moyens de preuve, lesquels sont appréciés souverainement par les juges du fond ».

La rationalité procédurale semble alors la meilleure piste à suivre. Confronté à un projet de dématérialisation de ce type, l'archiviste aura plus intérêt à convaincre les décideurs de l'utilité de bonnes pratiques permettant de limiter les risques d'irrecevabilité des preuves en cas de contentieux, que de chercher à déterminer si le projet est trop risqué pour être viable. Ces bonnes pratiques consistent essentiellement à :

- créer un faisceau de preuves ;
- penser en amont, avec le service juridique responsable de l'organisation en charge du contentieux, les modalités d'administration de la preuve à partir des documents et données numériques (copies d'écran, impression du document numérique avec impression de métadonnées, production du fichier électronique, voire recours à un huissier).

Créer un faisceau de preuves consiste avant tout à faire en sorte que le processus dématérialisé garantisse :

- la traçabilité des actions exécutées[1] ;
- le contrôle des accès aux systèmes d'information impliqués[2] ;
- la qualité du dispositif : il s'agit de pouvoir prouver que les dysfonctionnements sont traqués, repérés et supprimés et que, par conséquent, les données et documents qui y sont conservés sont fiables.

Ces exigences ne nécessitent pas forcément la mise en œuvre d'un système d'archivage électronique conforme à l'état de l'art : suivant la durée de conservation et les besoins de pérennisation à long terme des données considérées, un système d'information sécurisé ou un système de gestion électronique de documents incorporant un composant de coffre-fort électronique peuvent convenir[3].

---

[1] On pourra se reporter utilement à la norme NF Z 42-013 ainsi qu'à la note d'information du SIAF DGP/SIAF/2014/005 du 8 juillet 2014 relative à la journalisation des événements et à la note technique de l'ANSSI DAT-NT-012/ANSSI/SDE/NP du 2 décembre 2013 portant recommandations de sécurité pour la mise en œuvre d'un système de journalisation.

[2] On se reportera utilement aux nombreuses recommandations de l'ANSSI dans le domaine, que ce soit dans le RGS ou dans des documents spécifiques (voir http://www.ssi.gouv.fr/administration/bonnes-pratiques/).

[3] Décision n° 311095 du Conseil d'État, 5e et 4e sous-sections réunies, 31 mars 2008 : « l'apposition de la signature du sous-directeur de la circulation et de la sécurité routières au ministère de l'intérieur sur les décisions « 48 » et « 48 S » sous la forme d'un fac-similé, procédé inhérent à un traitement automatisé des décisions, identifie l'auteur de la décision et atteste que l'ensemble des informations qui y sont rapportées ont été enregistrées sous l'autorité et le

De la même façon, en dehors des documents évoqués dans la première partie de cet article, il est envisageable de prévoir la destruction, avant le terme de leur DUA, des documents originaux sur support papier après leur numérisation à condition que le processus de numérisation réponde aux exigences évoquées plus haut. C'est pourquoi le Service interministériel des Archives de France a publié un vade-mecum afin de guider les personnes en charge du contrôle scientifique et technique confrontées à de telles demandes d'élimination anticipée de documents papier[1]. Ce vade-mecum décrit concrètement les moyens techniques garantissant la constitution d'un faisceau de preuves à même d'emporter la conviction du juge en démontrant la fidélité de la copie numérique au document original.

Conclusion

Par cet article, je tenais à souligner le rôle particulier que l'archiviste peut essayer de jouer entre le juriste et l'informaticien. Il est maintenant rebattu de parler de la nécessaire collaboration entre archiviste et informaticien. J'insisterais plutôt sur la collaboration entre archiviste et juriste. Je parlerais même de la nécessité de l'archiviste de se perfectionner en droit car, par son habitude de la pratique et sa connaissance fine des besoins des administrations, il peut être un lien entre le décideur et le juriste, afin d'éviter que l'évaluation du risque juridique d'un projet de dématérialisation ne s'arrête à la première partie de cet article. L'archiviste a un rôle à jouer pour accompagner le besoin légitime de dématérialisation des organisations par des procédures qui limiteront le risque de voir les projets de dématérialisation se terminer par la chute de tout un système d'information après une jurisprudence défavorable.

Antoine MEISSONNIER
Adjoint au chef de bureau du contrôle et de la collecte des archives publiques
Service interministériel des Archives de France
antoine.meissonnier@culture.gouv.fr

contrôle du ministre de l'Intérieur dans les conditions prévues par le Code de la route et que la notification de chaque décision intervient à l'issue de l'ensemble des étapes rappelées ci-dessus ».

[1] Service interministériel des Archives de France, *Autoriser la destruction de documents sur support papier après leur numérisation. Quels critères de décision ?* mars 2014 : http://www.archivesdefrance.culture.gouv.fr/static/7429.