LE NUMERIQUE

GUIDE PRATIQUE

Application à la dématérialisation des contrats

Guide
des bonnes pratiques
du numérique

Application à la dématérialisation des contrats

Contributeurs au Groupe de Travail sur l'Economie Numérique (GTEN)

- *Chambre Monégasque des Nouvelles Technologies*
- *Association des Directeurs Informatiques de Monaco*
- *FedISA Monaco*
- *EuroCloud Monaco*
- *DataCenterMonaco*
- *Cabinet Giaccardi Avocats*

Palais de Monaco

Le 24 octobre 2014

C'est avec beaucoup d'intérêt que j'ai pris connaissance du projet de l'ensemble des associations et groupements composant le Groupe de Travail sur l'Economie Numérique de réaliser un guide des bonnes pratiques du numérique.

Le numérique constitue un enjeu stratégique pour Monaco, notamment dans la sensibilisation d'entreprises étrangères souhaitant s'y installer. Les acteurs locaux peuvent jouer un rôle essentiel en créant une synergie et des conditions favorables pour favoriser cet accueil.

Je souhaite féliciter l'ensemble des acteurs associés à cette dynamique pour leur implication dans un secteur d'activités qui se doit d'être un marché d'avenir, véhiculant une image moderne et dynamique de la Principauté.

SOMMAIRE

1 INTRODUCTION

Un constat s'impose désormais à nous, le numérique[1] nous envahit de plus en plus, à commencer par l'outil informatique mais également par le développement des réseaux de communication avec Internet et les services qui en découlent : commerce électronique, services en ligne, *cloud*, réseaux sociaux, … sans oublier la déferlante de terminaux nous permettant de nous connecter : ordinateur, smartphone et autres tablettes. En quelques années, le numérique est entré jusque dans nos foyers et n'est plus seulement l'apanage d'un environnement professionnel.

Là où il a fallu plusieurs siècles pour que le livre se diffuse, quelques dizaines d'années auront suffi aux smartphones pour s'imposer. Au-delà, la demande est désormais de plus en plus forte de pouvoir utiliser ses propres outils au travail, le fameux BYOD (Bring Your Own Device), ce qui ne va pas sans poser des difficultés en matière de sécurité dans son sens le plus large, mais aussi aux niveaux technique, juridique et personnel par rapport aux données échangées. Nous avons en réalité la chance de vivre une véritable révolution sociétale, plus forte encore et de beaucoup plus grande ampleur que la révolution industrielle du XIXème siècle, car à l'échelle mondiale.

Il s'agit en fait du résultat d'une évolution naturelle qui nous a permis de passer de l'informatisation, de l'automatisation à la dématérialisation dans son sens le plus étendu, à savoir la dématique. Contraction de dématérialisation et d'informatique, la dématique correspond ainsi à l'action de dématérialiser au sens large. Elle traite la numérisation de documents papiers, la dématérialisation des échanges et des processus métier en y incluant la composante légale, ainsi que la conservation sécurisée de l'ensemble des données/documents concernés.

Au sujet de la dématique (JM Rietsch)

L'utilisation du terme « dématérialisation » est source de nombreuses confusions, voire d'incompréhensions à cause d'une vision souvent incomplète du domaine. A noter également que nos amis anglo-saxons voient dans la « dematerialization » plutôt la notion de désintégration, ce qui n'est pas forcément le but recherché ! Nous proposons ainsi d'utiliser le mot « dématique » correspondant à l'action de dématérialiser dans son sens le plus large. La dématique va ainsi concerner à la fois la numérisation de documents, la dématérialisation des échanges et la dématérialisation des processus, sans oublier la prise en compte des aspects juridiques et réglementaires.

La première compréhension que l'on a en général de la dématérialisation est celle de la transformation du papier en électronique par le biais d'une opération classique de numérisation. Le document, une fois numérisé, sera ainsi accessible beaucoup plus facilement par un grand nombre d'utilisateurs. Il s'agit ici de la véritable origine et de l'objectif de la GED (Gestion Electronique de Documents), à ne pas confondre avec l'archivage électronique qui, dans la majorité des cas, concerne

[1] Le numérique (en anglais « digital ») correspond à un langage composé de chiffres : il s'agit d'un code. Par extension, on qualifie de « numérique » les machines (appareils photos, caméscopes, écrans plats, ordinateurs, téléphones, tablettes, ...) qui sont capables de comprendre ces langages, les informations (textes, photos, films, musiques...) qu'elles produisent ou qu'elles traitent et désormais les services associés. Le secteur du numérique désigne ainsi le secteur d'activité économique relatif aux Technologies de l'Information et de la Communication et à la production et à la vente de produits et services numériques.

des documents sur lesquels pèsent des obligations légales et/ou réglementaires nécessitant un niveau de sécurité élevé.

La dématique s'intéresse également à la dématérialisation des échanges, avec par exemple les e-mails ou encore les recommandés électroniques, le télétravail, les télé-procédures, en particulier administratives (déclarations d'impôts, de TVA).

Ce dernier point introduit naturellement le troisième aspect de la dématique qui concerne les processus pour lesquels le papier est totalement exclu. À titre d'exemple nous citerons la dématérialisation des factures, des contrats, des bulletins de salaires, …

Ce dernier volet de la dématique est celui qui présente le plus d'enjeux et correspond en fait à l'évolution naturelle de la démarche d'informatisation, à laquelle s'ajoute une dimension légale. La dématique doit ainsi permettre, en plus des procédures déjà connues et adaptées à l'électronique, d'envisager de nouveaux processus tout numériques qui vont permettre de pleinement profiter de l'électronique, gagnant en efficacité tant au niveau de la réduction des temps de traitement que de l'image de toute organisation publique ou privée au regard de ses clients, sans oublier la réduction de certains coûts.

Enfin, la dématique génère nécessairement un grand nombre de données/documents numériques et débouche naturellement sur la notion de conservation de ces mêmes données, posant un nouveau problème, celui de leur sécurité et surtout de leur pérennité.

L'aspect légal et réglementaire représente désormais une partie importante de ce genre de préoccupation en particulier pour la gestion et la protection des données personnelles. Ce qui montre bien qu'il ne s'agit pas seulement de problèmes purement techniques. Tout comme nous disposons d'une identité dans le monde physique, il est essentiel de pouvoir la traduire en une identité numérique qui nous permette de vivre dans ce nouveau monde numérique avec un maximum de confiance et sécurité. Ces deux derniers points sont essentiels pour permettre un développement durable du numérique qui ne pourra se faire que grâce à un environnement de confiance.

L'Europe ne s'y est pas trompée et le nouveau règlement européen du 23 juillet 2014 sur « *l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur* » résume bien dans son titre l'ensemble de la problématique. Plus dans le détail, il est intéressant d'y trouver les moyens d'une interopérabilité sécurisée pour l'ensemble des pays de l'Union en matière de numérique. On pourra en particulier citer la nécessité pour les pays de proposer un service d'authentification de leurs ressortissants accessible en ligne, l'interopérabilité des services publics et comme outils la signature électronique pour les personnes physiques, le cachet électronique pour les personnes morales, l'horodatage ou encore le recommandé électronique. A tout cela s'ajoute l'organisation des prestataires de service de confiance, également reconnus de façon transfrontalière.

Nouveau règlement européen sur la confiance (JM Rietsch)

Le 23 juillet dernier, l'Europe s'est dotée de son premier règlement destiné à offrir un maximum d'interopérabilité au niveau des Etats membres, sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, en lieu et place de la directive de 1999 sur un cadre communautaire pour les signatures électroniques. Contrairement à

une directive qui s'adapte aux différents droits nationaux, un règlement constitue l'équivalent d'une loi européenne et s'impose à l'ensemble des Etats membres.

Ce nouveau règlement tient compte à la fois du vécu de ces dernières années, tout en nous projetant dans l'avenir numérique. Il est d'ailleurs très significatif de constater qu'il commence par établir les bases d'une identification électronique et d'une authentification transfrontalière suivant différents niveaux (faible substantiel, élevé) à choisir en fonction de ses besoins. La qualité de l'identification constitue en effet l'un des fondements de la confiance dans un monde numérique et l'essentiel de la valeur d'une signature électronique, son lien avec la personne physique étant déterminant, quelle que soit la technique sous-jacente.

Afin de lever toute ambiguïté, la différence existe désormais clairement entre une signature électronique qui ne concerne que des personnes physiques et le cachet électronique réservé aux personnes morales sachant que la signature électronique d'une personne déléguée peut également jouer ce rôle. On notera également avec intérêt les précisions quant aux envois recommandés ainsi que sur les certificats électroniques d'authentification de site sans oublier l'ouverture à de nouveaux services essentiels comme la validation de la signature électronique et sa conservation.

L'organisation, la reconnaissance et le contrôle des prestataires de service de confiance ont également été particulièrement soignées et sont désormais gérées de façon transverse, même si certains services possèdent encore leurs propres exigences. La différence est principalement faite entre les prestataires de service de confiance qualifiés et les non qualifiés. Dans les faits cela se traduit côté utilisateur, par le renversement de la preuve et côté prestataire, par les garanties qu'il sera capable d'offrir en cas de dommage en fonction de sa solidité financière et d'une assurance adaptée.

L'aspect sécurité reste un élément essentiel et une importance particulière consiste à l'obligation de notifier tout incident en la matière, sans oublier la protection des données à caractère personnelle. A retenir enfin les obligations fortes pour le secteur public avec de vraies garanties offertes aux utilisateurs de tous ces services en particulier concernant l'aspect transfrontalier.

Applicable dès juillet 2016, ce règlement représente une étape extrêmement structurante en attendant le prochain règlement plus orienté sur la gestion des données à caractère personnelle.

Au-delà de ce constat que le numérique est désormais inéluctable il ne faut pas perdre de vue les enjeux stratégiques et prendre cette évolution comme une source de développement à tous les niveaux mais surtout ne pas rester au bord du chemin et savoir prendre le train en route. N'oublions pas également que le développement du numérique peut et doit avoir des conséquences en matière environnementale et de développement durable. En effet, même si de gros progrès restent à faire en matière de matériel informatique sur le sujet, force est de constater que petit à petit le volume de papier devrait largement diminuer avec un impact direct sur l'environnement, en particulier en matière de transport.

Comme toute nouveauté, le numérique porte avec lui son lot de contraintes et en premier lieu la nécessité de mettre en place une véritable gouvernance de l'information tant au niveau étatique qu'au niveau de chaque organisation avec comme principal objectif de valoriser cette précieuse information que l'on a trop souvent tendance à oublier pourtant partie prenante de notre patrimoine et de nos actifs.

Démathique et gouvernance : « La troisième plateforme » (JM Rietsch)

D'après IDC (International Data Corporation) l'univers numérique (on ne parle plus de monde) a bénéficié d'une croissance de 40% sur les dix dernières années passant de 132 exaoctets (10^{18}) de données créées et répliquées en 2005 à 4,4 zettaoctets (10^{21}) en 2013 pour atteindre 44 zettaoctets en 2020, soit un doublement tous les deux ans sachant qu'une grande partie de cette augmentation provient des objets connectés et autres terminaux « intelligents », sans oublier l'ensemble des échanges réalisés sur les réseaux sociaux.

Au-delà de ces chiffres que l'on a du mal à se représenter, la vraie question consiste à savoir comment sont exploitées ces données et l'on se rend alors bien compte de l'immense travail qui reste à accomplir en la matière.

En effet, toujours d'après IDC, seulement 22% de l'information de cet univers numérique pouvait prétendre être analysé en 2013, sous réserve d'avoir été marqué au préalable à l'aide majoritairement de métadonnées. En 2013, moins de 5% pouvait prétendre être étudié alors qu'en 2020, ce pourcentage pourrait monter à plus de 35%, principalement à cause de l'augmentation des données en provenance de systèmes intégrés qui génèrent automatiquement les métadonnées indispensables à un bon traitement ultérieur.

On nous annonce ainsi la « troisième plateforme » de l'âge numérique, bâtie sur la base du cloud computing, la mobilité, les réseaux sociaux et le Big Data.

D'un point de vue économique, le Boston Consulting Group prévoit que le numérique contribuera à concurrence de 4.200 milliards de dollars à l'économie des pays du G20 dès 2016, sachant qu'il représente d'ores et déjà une embauche sur deux aux Etats-Unis.

Une autre contrainte importante est représentée par la conduite du changement, à ne surtout pas négliger, au risque de voir échouer les projets. Cette conduite du changement se retrouve à tous les niveaux et en particulier celui de l'Etat, dont le rôle informationnel est absolument primordial dans l'environnement numérique.

Retenons enfin que la principale difficulté relève du caractère pluridisciplinaire du numérique à la fois technique, juridique et organisationnel et la nécessité d'aborder l'ensemble des problématiques traitées de façon transverse.

Quoiqu'il en soit le numérique représente une véritable révolution qui nous oblige à remettre en cause beaucoup de nos anciens schémas. Cependant soyons raisonnables, travaillons par étape et restons modestes sur certains projets, mais sachons profiter de cette formidable opportunité qui nous est offerte avec le numérique.

De l'appropriation et de l'absorption des nouvelles technologies (JM Rietsch)

Une récente étude IDC commanditée par EMC Corporation (leader mondial du stockage) nous révèle que l'environnement numérique a augmenté de 40% par an ces dix dernières années, sachant que cette augmentation touche aussi bien les données produites que le nombre de personnes et d'entreprises qui travaillent de façon connectée et tous les objets branchés correspondants. La taille des données numériques produites dans le monde atteint des valeurs encore inimaginables il y a seulement 30 ans.

Au-delà de l'émerveillement que cela entraine, la véritable question est de savoir finalement à quoi tout cela sert-il, est-ce vraiment efficace et n'est-on pas totalement dépassé par un phénomène de fuite en avant que plus personne ne maîtrise ? Ce phénomène est d'autant plus important qu'il touche tant l'espace professionnel que l'espace privé, pour preuve l'engouement pour les réseaux sociaux qui à eux seuls génèrent une masse considérable de données numériques et empiètent désormais également sur l'environnement professionnel.

Le numérique permet encore plus que d'autres technologies, de souligner le décalage entre les possibilités offertes par les techniques au sens large et leur utilisation au quotidien, notre capacité à se les approprier en tant qu'humain. Ainsi, en matière de dématique et d'informatique, même si le développement des nouvelles technologies s'arrêtait, nous en aurions encore au moins pour une génération afin de bien utiliser celles qui existent déjà de nos jours, et ce pour une large majorité d'entre elles. Un exemple très simple : qui d'entre nous peut aujourd'hui se targuer d'employer plus de 10% des capacités offertes par un traitement de texte ou encore plus par un tableur. De la même façon qui peut prétendre utiliser la majorité des capacités de son PC, voire de son smartphone ?

A peine commence-t-on à se sentir à l'aise avec un outil que déjà une nouvelle génération arrive et cela va encore en s'accélérant, en grande partie guidé par la poussée marketing sans que se pose encore la question des limites de capacité du marché à absorber toutes ces nouveautés.

Avant d'aller plus loin en matière technologique, il est urgent de développer l'utilisation de ces nouveaux outils au quotidien afin de ne pas risquer une véritable rupture entre la technique et les humains que nous sommes.

Au-delà de la conduite du changement et la lutte contre certaines réticences bien naturelles, il s'agit de rester raisonnable et d'éviter certaines affirmations comme celle de Bill Gates devant le think tank American Enterprise où il n'a pas hésité à dire que « dans vingt ans, les robots auront remplacés les chauffeurs, les serveurs et les infirmières ».

Ne sommes-nous pas là en train de confondre objectif technique et vie sociale ? Les réseaux sociaux nous ont déjà amené des centaines d'amis virtuels, espérons que le numérique ne nous conduira pas à une vie totalement virtuelle qui pourrait bien éteindre l'espèce, sans oublier que l'ensemble de ces cyber objets sont bien créés à l'origine par l'homme.

1.1 Situation de la Principauté

Compte tenu de sa taille et de son ralliement à l'Europe India Gateway (EIG), véritable autoroute de l'information virtuelle, la Principauté possède incontestablement la capacité à profiter pleinement des apports du numérique qui peuvent intervenir à deux niveaux :

- La modification/adaptation des processus : consiste à utiliser le numérique afin de simplifier mais surtout rendre plus efficaces des traitements déjà existants, tant dans le domaine public que privé. Il s'agit en fait de la poursuite de l'informatisation sur l'ensemble des processus en y intégrant la composante légale, la dématique ;

- Le développement de nouveaux outils et services directement liés aux capacités offertes par le numérique. Sur ce point, l'innovation reste le maître mot sans oublier le commerce électronique.

Une véritable volonté d'aller dans ce sens a ainsi été affichée par S.E.M. le Ministre d'Etat Michel Roger à l'occasion de la promulgation de la loi 1.383 sur le numérique en 2011, lorsqu'il a déclaré : « *La Principauté ne pouvait demeurer plus longtemps dénuée d'une législation propre à favoriser l'essor de l'économie numérique* ».

De même, Monsieur Alexandre Bordero, rapporteur du projet de loi, soulignait-il à l'époque : « *Cette loi est fondamentale. L'économie numérique est devenue un des secteurs majeurs du développement économique des sociétés contemporaines conduisant les pouvoirs publics à intégrer ce phénomène nouveau dans l'environnement juridique* ». Et l'élu de préciser que « *cela permettra à la Principauté de Monaco de conforter la croissance de ce secteur qui pourrait être dans un proche avenir, l'un des moteurs du dynamisme économique* ».

Les travaux sont en cours quant à la réalisation des ordonnances souverains relatives à cette loi et l'organisation à mettre en place de telle sorte que l'ensemble du dispositif devrait être prêt début 2015 en particulier en ce qui concerne les services et prestataires de confiance.

Rappelons que dans le domaine public, et depuis février 2011, la Principauté s'est dotée d'une Direction de l'Administration Électronique et de l'Information aux Usagers dont les principales missions sont :

- D'assurer le développement de l'Administration Électronique ;
- De rationaliser les procédures administratives en relation avec les Départements et Services administratifs ;
- D'assurer la gestion des demandes relatives aux procédures administratives, aux systèmes d'information et aux sites Internet issus des Départements et Services administratifs et leur concordance avec le schéma directeur ;
- De réaliser les actions d'assistance à la maîtrise d'ouvrage dans le cadre des projets informatiques ;
- De gérer les sites Internet du Gouvernement et d'assurer la cohérence d'ensemble du paysage Internet de l'Administration ;
- De mettre à disposition des usagers une documentation administrative complète et les informer sur les démarches à accomplir ;
- D'identifier et analyser les attentes des usagers en matière de procédures et d'information administratives.

Actuellement, il n'y a toujours pas de signature numérique en Principauté et aucune entité pour gérer ce genre de procédé, pourtant indispensable à l'instauration d'un environnement de confiance autour et pour le numérique.

☛ Il y aurait lieu de tout de suite travailler à une évolution de la loi en particulier, afin de l'étendre aux services financiers qui en sont actuellement partiellement exclus, et surtout de prévoir la possibilité de supprimer le papier après numérisation avec une notion essentielle de transfert d'original, ce qui en Principauté serait source d'un gain très important en espace et répondrait ainsi à un besoin exprimé par bon nombre des acteurs économiques de la place.

1.2 Positionnement du GTEN

Fort de ce qui précède, le GTEN s'est donné pour mission de participer et surtout d'aider à ce développement plus particulièrement dans le domaine privé. Ce guide constitue une première étape destinée à poser les bases d'un processus dématérialisé et surtout à décrire les outils indispensables pour un fonctionnement efficace et sécurisé à tous les niveaux, y compris légaux.

Du point de vue méthodologique, lorsqu'il s'agit de dématérialiser un processus, il existe trois façons d'aborder le sujet, à savoir :

- Calquer purement et simplement le nouveau processus sur l'ancien avec un double risque qui est celui de perdre en efficacité au final et surtout de mettre en place des outils mal dimensionnés ;
- Revoir le processus dans son ensemble afin de l'adapter au mieux aux nouvelles technologies mise en œuvre ;
- En profiter pour s'organiser !

Bien évidemment nous recommandons de travailler à partir de la deuxième proposition même si dans la réalité la première est de loin la plus courante.

Un maître mot s'impose lorsque l'on traite de la dématérialisation d'un processus, celui de cycle de vie qui doit s'appliquer à tout document numérique et qui va permettre de suivre l'évolution dudit document tout au long de son existence comme nous le verrons ultérieurement.

2 PREAMBULE

Avant d'entrer dans le détail d'un processus dématérialisé, il nous semble nécessaire d'insister et de préciser ici l'importance à apporter à la notion d'identité numérique et à celle de sécurité de l'information et des données personnelles.

2.1 Identité numérique

L'identité numérique peut être définie comme un lien technologique entre une entité réelle (la personne) et une entité virtuelle (sa ou ses représentation(s) numériques). Les réseaux sociaux et les blogs ont provoqué la prolifération des données personnelles et chaque utilisateur doit désormais gérer une véritable « identité numérique » constituée des informations qu'il a saisies dans ses profils, de ses contributions (par exemple dans les blogs) et des traces laissées sur les sites. Il est du rôle régalien de l'Etat de faire en sorte que chaque citoyen puisse disposer d'une identité numérique légitime, garantie par son pays, libre à lui ensuite d'en utiliser d'autres en fonction de ses besoins.

Sur ce point, la Principauté a été en pointe en 2009 avec le lancement de sa carte d'identité électronique, la première au format ECC (European Citizen Card). Malheureusement réservée aux seuls citoyens monégasques, le développement des services autour de ce mode de contrôle de l'identité numérique, n'a pu encore être entamé.

☞ Afin d'étendre les possibilités offertes par la CIME (Carte d'Identité Monégasque Electronique) à la quasi-totalité des personnes œuvrant en Principauté l'on pourrait envisager la modification de la carte de résident, ainsi que celle des travailleurs étrangers, voire reprendre l'actuel permis de travail.

De l'identité numérique et du rôle des Etats (JM Rietsch)

Le principal risque lié au cloud vu comme un espace planétaire de stockage et de traitement de données numériques, se situe au niveau de la protection de ces mêmes données dans la mesure où il faut être averti et surtout conscient de l'utilisation qui pourrait en être faite par les opérateurs de service, notamment en termes d'analyse et en particulier au niveau du comportement. L'on découvre ainsi par exemple qu'un amateur de musique de jazz le serait également de romans policiers, d'où les propositions commerciales qui en découlent ! Il serait utopique de vouloir protéger et réglementer sur le sujet au niveau international, mais les États peuvent cependant garantir des espaces protégés à un niveau national, espace privilégié où l'utilisateur sait qu'aucun traitement ne sera fait sans son consentement et où ses données seront réellement protégées.

Le cloud est lié à un autre domaine absolument essentiel : celui de l'authentification au sens de l'identité numérique. En effet, l'usurpation d'identité est un fléau aux conséquences dramatiques pour les victimes. Si le vol de carte bancaire a déjà des conséquences dommageables, des risques beaucoup plus grands existent quand c'est toute l'identité de la personne qui est usurpée, la carte bancaire ayant un plafond de dépenses, l'identité n'en ayant pas. La gestion de l'identité numérique constitue donc un problème technique et organisationnel aux implications juridiques énormes, qui doit trouver des solutions pour permettre le développement sécurisé du cloud et de tout l'univers numérique. Plusieurs approches existent aux niveaux technique et organisationnel.

Dans le monde numérique, il n'est pas rare d'avoir plusieurs solutions à un même problème, présentant chacune ses avantages et ses inconvénients, en particulier au niveau de la sécurité. La véritable difficulté est ainsi d'adapter la solution technique à ses besoins. Cependant, attention au fait

que le trop devient très vite l'ennemi du bien. Plus on élève le niveau de sécurité, plus on augmente les contraintes, d'où un fort risque de non-respect ou de contournement. Pour un petit achat par exemple, une authentification par SMS pourra suffire, mais cela ne sera pas le cas pour un achat de plusieurs dizaines de milliers d'Euros, qui demandera une authentification beaucoup plus forte. Idéalement l'utilisateur devrait être conscient des avantages et inconvénients de chaque solution et choisir en fonction du degré de protection dont il a réellement besoin. Il est essentiel de nos jours que l'utilisateur tant privé que professionnel soit bien averti et prenne conscience de ces différences et assume sa responsabilité face aux choix techniques et organisationnels.

L'État a un rôle important à jouer en matière d'identité numérique dans la mesure où il s'agit là d'un domaine régalien comme pour les Cartes d'Identité ou les Passeports.

2.2 Sécurité de l'information et données personnelles

Le thème de la sécurité de l'information n'est pas nouveau mais revêt désormais une acuité particulière du fait de l'augmentation des volumes d'information produits, échangés et surtout conservés. En effet, l'évolution d'Internet offrant de plus en plus de services pour les particuliers, les entreprises et les gouvernements, amène immanquablement à se poser la question de la sécurité de l'information et plus particulièrement des données personnelles. La Principauté ne s'y est pas trompée et en matière de sécurité a lancé récemment la création d'un CERT. En ce qui concerne les données personnelles, rappelons qu'il s'agit là de la mission de la CCIN (Commission de Contrôle des Informations Nominatives)[2].

Là encore les réponses à ces problématiques sont pluridisciplinaires et en particulier concernent les aspects :

- **Techniques :** technologies à mettre en œuvre pour gérer l'identité ;
- **Psychologiques et sociaux :** la projection de l'identité en ligne revêt des enjeux nouveaux, comme la demande de droit à l'oubli (pouvoir effacer des contenus sur Internet) ;
- **Légaux :** le droit se fondant sur les définitions de personnes physiques et morales, il a connu quelques adaptations pour renforcer la notion d'identité et son applicabilité dans l'ère du numérique ;
- **Éducatifs :** étant donné l'accès des plus jeunes aux technologies de l'information et de la communication et la permanence des traces laissées sur les réseaux, la prévention par la sensibilisation des utilisateurs.

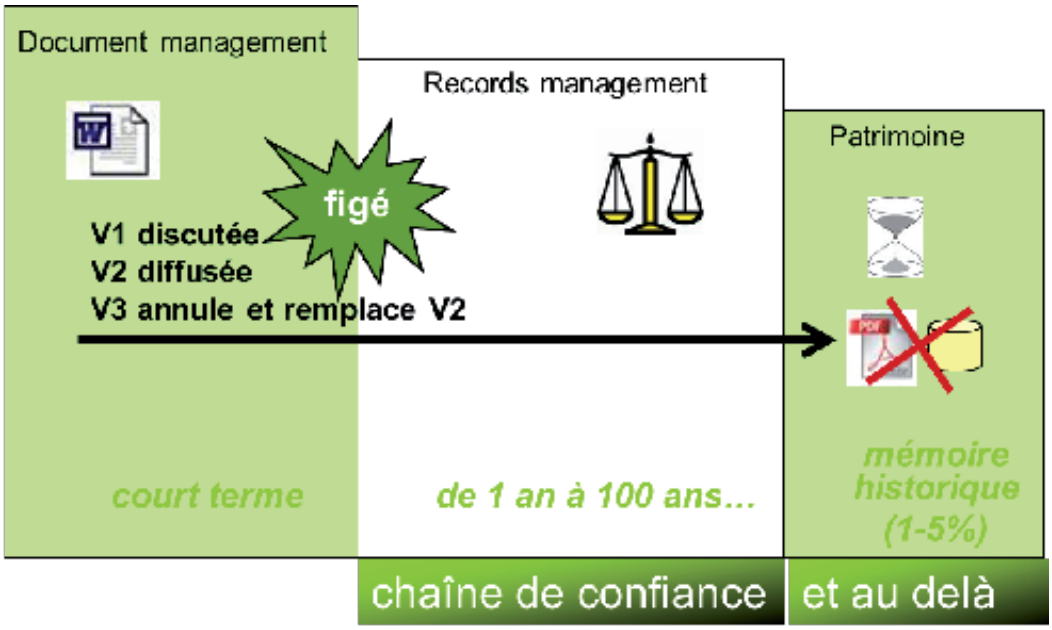
Cette notion de sensibilisation est absolument essentielle du fait que l'Etat, dans son rôle de protection de ses citoyens, se doit dans un environnement numérique en perpétuel évolution, d'informer ses citoyens des dangers potentiels, les lois à elles seules ne pouvant assurer une complète sécurité dans la mesure où le numérique n'a pas de frontière et lorsque le mal est fait, il est souvent trop tard : mieux vaut prévenir que guérir.

[2] La CCIN a pour mission de veiller au respect des libertés et droits fondamentaux des personnes dans un domaine particulier : l'utilisation de leurs informations personnelles. Elle s'assure ainsi que l'exploitation informatique qui en est faite ne porte pas atteinte à la vie privée des justiciables, à leur liberté d'aller et de venir, à leur liberté de conscience…

3 PROCESSUS DEMATERIALISE

3.1 Cycle de vie du document

Le schéma présenté ici montre les trois grandes étapes de la vie d'un document à savoir de sa création à sa validation, sa première phase de conservation pour des raisons essentiellement légale et réglementaire, et enfin sa suppression ou la poursuite de sa conservation à des fins plutôt historiques et patrimoniales.



La notion de « figé » correspond au moment où un document est validé et ne doit plus être modifié. Cette étape est malheureusement souvent difficile à identifier à l'intérieur des systèmes d'information actuels alors que la sécurité du document doit être assurée dès cet instant.

Nous détaillons ci-dessous la première partie du cycle de vie du document afin de montrer les différents éléments à prendre en compte, tant au niveau de la multiplicité des formats que l'on peut rencontrer que des plateformes informatiques à traverser, sans oublier les personnes concernées dont le consentement sera nécessaire.

L'objectif final consiste à disposer à la fin de cette première phase d'un document validé tant par son origine que par la conformité vis-à-vis de son établissement. Arrive ensuite la phase de conservation du document accompagné des traces correspondantes. Le dispositif utilisé devra alors garantir le caractère authentique du document, à la fois son intégrité et son origine sans oublier son intelligibilité et ce pendant toute la durée de conservation qu'elle soit légale ou non.

3.2 Exemple du flux signature d'un contrat

L'ensemble des contrats peut se traiter de façon totalement numérique, y compris les actes authentiques pour les notaires et les huissiers. Les gains issus de cette dématérialisation sont très importants et se retrouvent à plusieurs niveaux. Tout d'abord en matière d'efficacité car la réalisation du contrat est en générale plus rapide, mais aussi en recherche dans la mesure où l'on dispose d'un exemplaire numérique unique et non de plusieurs copies papiers dont on a souvent du mal à extraire la bonne. Ensuite en matière de coûts, la finalisation d'un contrat numérique est moins onéreuse que dans un environnement papier de par une plus grande rapidité d'exécution, voire une économie directe en matière d'affranchissement et surtout de stockage.

Les grandes étapes génériques du processus de signature d'un contrat sont les suivantes :

1. Elaboration contrat (personnalisé en fonction du client)
2. Signature des parties
3. Conservation sécurisée

Un certain nombre de points de vigilance sont à prendre en compte à chaque étape que nous allons reprendre plus en détail ci-après.

3.2.1 Elaboration d'un contrat

Le suivi du flux doit permettre d'identifier :

- Les différentes plateformes informatiques afin de vérifier la sécurité au sein de chacune et la sécurité des transferts entre plateformes
- Les formats logiques utilisés, Microsoft Word, Adobe PDF, …
- Les intervenants en tant que personne physique ou représentant une entité, voire une personne morale en tant que telle

☞ Objectif : **Garantir l'intégrité du document, identifier les traitements et les intervenants**

3.2.2 Signature des parties

Dans la mesure où l'on a recours à la signature électronique il faudra vérifier :

- Le mode de délivrance des certificats électroniques
- La qualité de l'outil de signature
- Le format de signature utilisé

- La qualité des plateformes en particulier si l'on s'adresse à des prestataires externes

☞ Objectif : **Garantir le lien entre les différentes personnes et le document**

3.2.3 Conservation sécurisée

Lorsque le contrat est signé plusieurs opérations restent à réaliser pour sa conservation :

- La validation des signatures qui consiste à vérifier la qualité de la signature d'un point de vue juridico-technique
- Le transfert vers une plateforme de conservation, éventuellement chez un prestataire tiers
- La conservation sécurisée et pérenne

☞ Objectif : **Garantir le caractère authentique du document, sa pérennité et son intelligibilité**

3.2.4 Traces

La constitution des traces doit permettre à chaque étape importante d'avancement du document de répondre aux différentes questions suivantes sur toutes les plateformes :

- Qui, quoi, quand ?
- Ordre des validations éventuelles des documents utilisés/présentés

☞ Objectif : **Garantir la séquentialité et la complétude des opérations du cycle de vie du document**

De ce qui précède apparaît clairement la nécessité de disposer des outils de base que sont :

- La signature électronique
- L'horodatage
- L'archivage sécurisé
- La validité, la « preuve »

Que nous allons maintenant détailler.

4 SIGNATURE ELECTRONIQUE

4.1 Définition

Qu'est-ce que la signature électronique ?

Il s'agit tout d'abord d'un concept, mêlant des aspects pratiques, juridiques et techniques. En résumé, la signature électronique est un procédé technique dans lequel une personne (le signataire) appose son accord à valeur juridique sur un document électronique. Dans un cas (électronique) comme dans l'autre (manuscrite), il y a donc réunion de 3 items : le document, le signataire et l'outil de signature.

Ce dernier point représente généralement la plus grande difficulté de compréhension au non-initié. Car si l'outil nécessaire à la signature manuscrite n'est ni plus ni moins qu'un stylo, les outils de signature électronique sont multiples, autant que les moyens techniques nécessaires à leur réalisation. Concrètement, il s'agit dans la majorité des cas d'un certificat numérique porté sur différents supports (carte à puce, clé USB, carte d'identité, PC, smartphone, etc.) et qui a pour fonction d'identifier le signataire d'une part, et de sceller le document pour en garantir l'intégrité d'autre part tout en assurant le lien entre les deux.

Le **règlement UE du 23 juillet 2014** sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur précise que l'effet juridique d'**une signature électronique qualifiée est équivalent à celui d'une signature manuscrite**.

Dans ce règlement, on entend par :

- **«signataire»**, une personne physique qui crée une signature électronique;
- **«signature électronique»**, des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique et que le signataire utilise pour signer;
- **«signature électronique avancée»**, une signature électronique qui satisfait aux exigences énoncées à l'article 26 du règlement,
- **«signature électronique qualifiée»**, une signature électronique avancée qui est créée à l'aide d'un dispositif de création de signature électronique qualifié (exigences dans article 29 du règlement), et qui repose sur un certificat qualifié de signature électronique.

Au sujet de la signature électronique en France (Eric Barbry)

La signature électronique a déjà eu deux vies… elle est en train d'en connaître une troisième…

Née en 1989 ou presque, à l'occasion d'une décision de la Cour de cassation (Arrêt Crédicas), la première vie de la signature électronique est d'ordre jurisprudentiel. Sans cadre règlementaire, elle n'est alors reconnue que par le juge qui la combine avec la « convention de preuve », c'est-à-dire la faculté qu'on les parties contractantes de déterminer ensemble les preuves qu'elles voudront s'opposer.

En 2000, la signature entre dans une nouvelle ère. Elle se voit reconnaître un statut légal consacré par une modification du Code civil et l'ajout d'un article 1316-4 alinéa 2 qui dispose : « Lorsqu'elle est électronique (i.e. la signature), elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat…. ».

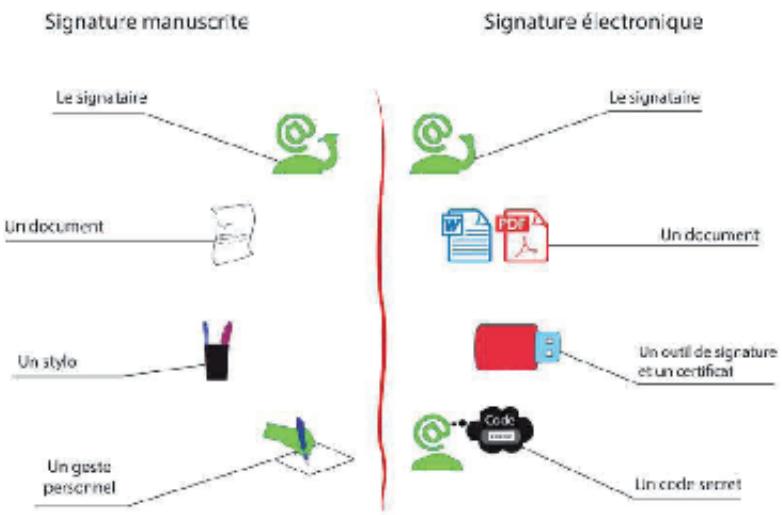
Malgré cette avancée indiscutable, la signature électronique ne connaît pas le développement attendu. Elle était en effet jugée trop complexe tant sur un plan pratique que sur un plan juridique. Il est vrai que le droit de la signature électronique n'est pas un droit des plus digestes !

La signature électronique connaît depuis quelques années un développement nouveau. Il s'est accéléré depuis quelques mois suite principalement à la décision de la Cour d'appel de Nancy du 14 février 2013.

Ce développement s'explique notamment par le fait, d'une part, d'un déploiement quasi imposé aux entreprises (télé-déclaration, comptabilité numérique, marchés publics, ...) et une technologie plus aisée notamment supportée par la tablette graphique. Dans certains secteurs d'activités ou pour certaines fonctions, la signature électronique est devenue la manière « normale » de signer un acte (avocat, médecins, élus d'une collectivité, DAF, etc, …).

Face à ce retour en force de la signature électronique, il est important que les entreprises publiques ou privées se repositionnent et s'interroge sur leur propre « passage » à la signature électronique.

Définition schématique et pratique :



Dans le cas ci-dessus, la signature est réalisée par une personne physique. Ce principe peut également être employé de manière identique dans des contextes juridiques et fonctionnels différents, pour obtenir des « signatures électroniques » au sens technique, mais ayant une portée et un usage très différent : la signature de personne morale ou de serveur (aussi appelée « cachet »), et les différents usages de la signature à des fins purement techniques. On parlera alors de « scellement » et non de « signature ».

Définition AFNOR :

La signature électronique est un mécanisme permettant de garantir l'intégrité d'un document électronique et d'en authentifier l'auteur, par analogie avec la signature manuscrite d'un document papier.

L'authentification repose sur l'utilisation de la technologie de la cryptographie.

Avec l'intensification des échanges électroniques et des projets de dématérialisation, la signature électronique est en fort développement.

Les différents modes de réalisation de la signature électronique

En fonction des contraintes liées au projet et aux signataires, il est possible d'envisager des manières très différentes de réaliser la signature électroniques.

Nous allons ici en décrire quatre, qui sont les plus répandues, mais qui ne sauraient être exhaustives.

La signature électronique « autonome »

Dans ce mode de réalisation, le signataire dispose sur son poste de travail d'un logiciel de signature électronique, ainsi que d'un certificat qu'il a acquis auprès d'une Autorité de Certification, par exemple sous la forme d'une carte à puce.

Le certificat nécessite une installation sur le poste de travail, mais cette installation est réalisée une seule fois, suite à quoi le signataire peut se servir de son certificat sans aucune contrainte technique.

Après avoir démarré le logiciel de signature, le signataire sélectionne le document à signer.

Le logiciel accède alors à la carte à puce et demande la saisie du code PIN.

Une fois le code PIN saisi, la signature électronique est réalisée dans la carte à puce, puis transmise au logiciel qui en fera la mise en forme selon le format attendu.

L'utilisateur est, dans ce cas, totalement autonome pour réaliser des signatures électroniques.

C'est notamment le choix qui a été fait pour la signature électronique des experts-comptables, Signexpert.

La signature électronique via une applet

Dans ce mode de réalisation, le signataire dispose sur son poste de travail uniquement d'un certificat qu'il a acquis auprès d'une Autorité de Certification, par exemple sous la forme d'une carte à puce.
Le certificat nécessite une installation sur le poste de travail, mais cette installation est réalisée une seule fois, suite à quoi le signataire peut se servir de son certificat sans aucune contrainte technique.

Le service dans lequel la signature est nécessaire contient un programme téléchargeable appelé une « applet ». Lorsque l'utilisateur doit signer, cette applet est automatiquement chargée sur son poste et exécutée.

Le document à signer est présenté à l'utilisateur qui confirme sa volonté de signer. L'applet accède alors à la carte à puce et demande la saisie du code PIN. Une fois le code PIN saisi, la signature

électronique est réalisée dans la carte à puce, puis transmise à l'applet qui en fera la mise en forme selon le format attendu.

Dans ce cas, l'utilisateur dispose d'un certificat qu'il pourra employer dans divers services, sans avoir besoin sur son poste d'un logiciel de signature électronique, puisque ce logiciel (l'applet) lui est transmis à chaque besoin. La signature reste sous son contrôle exclusif puisque, sans saisie du code PIN, elle ne pourra pas être réalisée.

Le format de la signature électronique est choisi par l'applet en fonction du service dans lequel elle s'exécute, de manière transparente pour le signataire.

C'est notamment le choix qui a été fait par la majorité des plates-formes de réponse aux marchés publics.

La signature électronique « à la volée »

Dans ce mode de réalisation, le signataire dispose uniquement d'un moyen d'authentification, qui lui permettra de prouver son identité vis-à-vis de la plate-forme.

Il pourra s'agir par exemple d'un numéro de téléphone mobile sur lequel il recevra un code à usage unique, qu'il devra ressaisir.

Le service dans lequel la signature est nécessaire présente à l'utilisateur le document à signer. Lorsque l'utilisateur confirme sa volonté de signer, le procédé d'authentification du signataire se déclenche (par exemple par l'envoi d'un SMS).

Une fois le signataire authentifié, la plate-forme de service (ou un Tiers de Confiance auquel elle fait appel) génère un certificat au nom du signataire, réalise elle-même la signature électronique, puis détruit la clef privée correspondante de manière à garantir qu'elle ne soit utilisée qu'une fois.

Le document signé peut alors être envoyé au signataire ou mis à sa disposition. Dans ce cas, aucune contrainte d'usage n'est imposée au signataire : ce procédé est d'une grande souplesse et d'une grande ergonomie pour l'utilisateur.

Le niveau de sécurité de la signature sera celui du procédé d'authentification employé. Saisie d'un mot de passe ou d'un code à usage unique.

C'est notamment le choix qui a été fait par de nombreux services de contractualisation en ligne.

La signature électronique par « carte à puce virtuelle »

Dans ce mode de réalisation, comme pour la signature électronique à la volée, le signataire dispose uniquement d'un moyen d'authentification, qui lui permettra de déclencher l'utilisation de son certificat par la plate-forme.

Un certificat permanent au nom du signataire est généré en amont de l'utilisation du service, mais au lieu d'être remis au titulaire comme dans le cas de la signature électronique autonome, ou d'être temporaire comme dans le cas de la signature électronique à la volée, il est conservé sur le serveur au sein d'un module cryptographique physique (HSM pour Hardware Security Module) : ce module constitue une « carte à puce virtuelle ».

Le service dans lequel la signature est nécessaire présente à l'utilisateur le document à signer. Lorsque l'utilisateur confirme sa volonté de signer, le signataire transmet son code de déblocage qui permet à la carte à puce virtuelle de réaliser la signature électronique. Le document signé peut alors être envoyé au signataire ou mis à sa disposition.

Dans ce cas, aucune contrainte d'usage n'est imposée au signataire : ce procédé est d'une grande souplesse et d'une grande ergonomie pour l'utilisateur.

Le niveau de sécurité de la signature dépendra du mode de délivrance du certificat dans la carte à puce virtuelle, et de la sécurisation de la transmission du code de déblocage.

C'est notamment le choix qui a été fait par de nombreux services de contractualisation en ligne où l'usager revient de manière récurrente.

La fiabilité de l'identité numérique

La confiance que l'on peut avoir dans une identité numérique sera fonction du processus d'enregistrement (ou d'enrôlement) mis en œuvre pour l'établir.

Aux débuts de l'histoire de la signature électronique, VeriSign, acteur technique de la certification, a défini trois niveaux d'enregistrement, appelés « classes » :

• **classe 1** : certification de l'identité d'un signataire sans autre contrôle que la validité de son adresse mail ;

• **classe 2** : certification de l'identité d'un signataire à distance, sur la base de copies de ses papiers d'identité ;

• **classe 3** : certification de l'identité d'un signataire suite à une rencontre en face à face, et sur présentation des papiers d'identité originaux.

Un symbole « + » est ajouté à la classe pour mentionner le fait que le certificat d'identité délivré est hébergé sur un support cryptographique physique : carte à puce ou clef USB contenant un certificat.

4.2 Utilisations

Dans quelles situations utilise-t-on la signature électronique ?

Toutes, dès lors que le document à signer est lui-même dématérialisé : un contrat, un avenant à un contrat, un paiement, une prescription médicale, etc. Le cas de l'abonnement en ligne est un bon exemple : en règle générale, une fois l'inscription enregistrée sur le site du prestataire, les documents à signer sont envoyés par courrier à l'abonné, qui les signe et les renvoie. Avec la signature électronique, tout pourrait être signé et finalisé en quelques minutes et à distance.

D'ailleurs, la signature électronique est d'ores et déjà utilisée dans certains cas, parfois même sans que le signataire n'en ait conscience : c'est le cas notamment de la saisie d'un code reçu par SMS pour valider un paiement par exemple. En soi, la transmission de ce code active un certificat numérique dit « à la volée » (unique) et, à ce titre, vaut signature électronique.

Mais de nombreux autres usages pourraient être imaginés, notamment dans des corps de métiers où l'engagement – et donc la signature – est très présent. En particulier dans les professions juridiques, médicales.

Justement, certains secteurs sont-ils plus porteurs que d'autres en la matière ?

Les professions juridiques telles que les avocats et les huissiers ont déjà fait beaucoup de progrès, notamment dans la transmission des actes. Les notaires également, avec une particularité : en raison des implications des actes notariés en matière immobilière comme familiale, la présence physique de la personne est généralement exigée, même pour une signature électronique.

Dans d'autres cas, ce sont des dispositions légales qui ont imposé la signature électronique. C'est le cas par exemple des réponses à appels d'offres publiques, qui réunissent l'obligation de dématérialisation en même temps qu'une obligation de signature : les répondants doivent donc obligatoirement se munir d'un certificat numérique pour répondre.

D'autres secteurs sont également très actifs en matière de signature électronique : la formation (signature des conventions et des documents de présence), l'assurance, la banque, la santé, ... La législation SEPA (Single Euro Payments Area) devrait accélérer le mouvement dans le monde bancaire avec l'obligation de signature de certains virements. Le monde de la santé met en place des solutions adaptées pour favoriser la circulation des informations entre les professionnels de santé.

Que peut-on signer électroniquement ?

Le mécanisme technique de signature électronique ne dépend pas du format des données que l'on souhaite signer : il est ainsi possible de réaliser une signature sur un document bureautique, une image, une vidéo, des données brutes ou tout autre fichier informatique, quel qu'en soit la nature.

Toutefois, lorsque la signature électronique est employée pour recueillir l'engagement du signataire, il est préférable de la faire porter sur un document intelligible par un être humain !

Certains cas d'usage méritent d'être précisés :

• Signer électroniquement un zip n'équivaut pas à signer électroniquement chacun des documents contenus dans le zip : il convient de réaliser la signature de chacun des documents avant de constituer le zip qui contiendra les documents et leurs signatures.

• Le format S/MIME permet de signer électroniquement les courriers électroniques. De même que pour un zip, signer électroniquement un mail contenant une pièce jointe n'est pas équivalent à l'envoi par mail d'une pièce jointe signée.

Vérifier une signature électronique

Une différence fondamentale entre la signature électronique et la signature manuscrite est la faculté à la vérifier avec certitude… Faculté qui devient même une obligation à chaque usage d'un document signé électroniquement !

La vérification d'une signature électronique nécessite trois étapes :

a. La vérification technique de la signature

Elle consiste à vérifier les aspects cryptographiques de la signature.

Si elle est la plus complexe techniquement, elle est la plus simple en pratique, car elle est entièrement prise en charge par les outils.

b. La vérification de la chaîne de confiance

Elle consiste à vérifier la validité du certificat du signataire, sa non révocation, le certificat de l'Autorité de Certification émettrice, et le fait que cette Autorité de Certification soit référencée dans une liste officielle, ou soit acceptée dans la Politique de Signature Electronique du service incluant la vérification.

Cette étape est également en grande partie automatisée. Ces deux étapes sont largement simplifiées en électronique par rapport à la signature manuscrite.

c. La vérification de l'habilitation du signataire

Cette ultime étape consiste à s'assurer que le signataire, dont l'identité a été garantie par les étapes précédentes, avait bien le droit de signer l'acte dont la signature est en cours de vérification. Cette vérification peut se faire au travers de plusieurs méthodes : une liste de signataires habilités prédéfinie, la vérification du Kbis de l'entreprise d'appartenance du signataire, l'existence d'une délégation de pouvoir lui concédant l'habilitation (dont la validité doit aussi être vérifiée !)… C'est dans la pratique la vérification la plus complexe à faire car elle est soumise à l'interprétation humaine. Mais cette vérification n'est pas spécifique à la signature électronique, elle doit aussi être réalisée pour une signature manuscrite.

d. Exigences applicables à la validation des signatures électroniques qualifiées (règlement européen)

Le processus de validation d'une signature électronique qualifiée confirme la validité d'une signature électronique qualifiée à condition que:

- le certificat sur lequel repose la signature ait été, au moment de la signature, un certificat qualifié de signature
- le certificat qualifié ait été délivré par un prestataire de services de confiance qualifié et était valide au moment de la signature;
- les données de validation de la signature correspondent aux données communiquées à la partie utilisatrice.
- l'ensemble unique de données représentant le signataire dans le certificat soit correctement fourni à la partie utilisatrice;
- l'utilisation d'un pseudonyme soit clairement indiquée à la partie utilisatrice, si un pseudonyme a été utilisé au moment de la signature;
- la signature électronique ait été créée par un dispositif de création de signature électronique qualifié;
- l'intégrité des données signées n'ait pas été compromise;

- les exigences prévues à l'article 26 aient été satisfaites au moment de la signature.
- Le système utilisé pour valider la signature électronique qualifiée fournit à la partie utilisatrice le résultat correct du processus de validation et permet à celle-ci de détecter tout problème pertinent relatif à la sécurité.

e. Service de validation qualifié des signatures électroniques qualifiées (règlement européen)

Un service de validation qualifié des signatures électroniques qualifiées ne peut être fourni que par un prestataire de services de confiance qualifié qui :

- fournit une validation conforme; et permet aux parties utilisatrices de recevoir le résultat du processus de validation d'une manière automatisée, fiable, efficace et portant la signature électronique avancée ou le cachet électronique avancé du prestataire qui fournit le service de validation qualifié.

La Commission peut, au moyen d'actes d'exécution, déterminer les numéros de référence des normes applicables au service de validation qualifié. Le service de validation de signatures électroniques qualifiées est présumé satisfaire aux exigences fixées. Ces actes d'exécution sont adoptés en conformité avec une procédure d'examen.

Conserver des documents signés électroniquement

Un service de conservation qualifié des signatures électroniques qualifiées ne peut être fourni que par un prestataire de services de confiance qualifié qui utilise des procédures et des technologies permettant d'étendre la fiabilité des signatures électroniques qualifiées au-delà de la période de validité technologique.

4.3 Agrément (règlement européen)

Le règlement européen prévoit que la conformité des dispositifs de création de signature électronique qualifiés avec les exigences fixées en annexe, est certifiée par les organismes publics ou privés compétents désignés par les États membres.

Les États membres notifient à la Commission, dans les meilleurs délais et au plus tard un mois après la conclusion de la certification, des informations sur les dispositifs de création de signature électronique qualifiés qui ont été certifiés par les organismes compétents qu'ils ont désignés.

Ils notifient également à la Commission, dans les meilleurs délais et au plus tard un mois après l'annulation de la certification, des informations sur les dispositifs de création de signature électronique qui ne sont plus certifiés.

Sur la base des informations reçues, la Commission établit, publie et met à jour une liste des dispositifs de création de signature électronique qualifiés certifiés.

Les mêmes exigences et les modalités de publication s'appliquent également aux dispositifs de création de cachet électronique.

5 HORODATAGE

5.1 Définition de l'horodatage

Le règlement européen stipule dans son chapitre 1, article 3 "Définitions", alinéa 33 : "Horodatage électronique, des données sous forme électronique qui associent d'autres données sous forme électronique à un instant particulier et établissent la preuve que ces dernières données existaient à cet instant". Dans son article 34, il précise également : "*L'horodatage électronique qualifié, un horodatage électronique qui satisfait aux exigences fixées à l'article 42*". Cet article 42 définit les exigences applicables aux horodatages électroniques qualifiés, à savoir :

a) il lie la date et l'heure aux données de manière à raisonnablement exclure la possibilité de modification indétectable des données;
b) il est fondé sur une horloge exacte liée au temps universel coordonné; et
c) il est signé au moyen d'une signature électronique avancée ou cacheté au moyen d'un cachet électronique avancé du prestataire de services de confiance qualifié, ou par une méthode équivalente[3].

5.2 Utilisations de l'horodatage

Un procédé d'horodatage peut être utilisé pour apposer une date d'expédition ou de réception d'un courrier, mais plus largement pour attester de l'existence d'une donnée à un instant ou de la date d'un acte réalisé par voie électronique.

Voici quelques exemples d'utilisations :

- Scellement de logs informatiques à des fins probatoires ;
- Datation d'une signature électronique ;
- Validation de l'heure de réception d'un pli sous forme électronique ;
- Certification de transactions bancaires ;
- Apposition d'une date d'émission sur une facture électronique ;
- Clôture d'une enchère électronique ;
- Attestation de dates d'émission ou de réception d'e-mail ;
- Séquencement des transactions sur une plate-forme d'échanges électronique.

Lorsque vous envoyez des fichiers dessins sur Internet ou travaillez sur des projets de groupe, vous pouvez recourir à un serveur spécifique afin de créer une référence de temps cohérente.

[3] Il est intéressant de constater que par ces mots, l'UE prévoit que l'innovation pourrait déboucher sur de nouvelles technologies susceptibles d'assurer un niveau de sécurité équivalent pour la signature électronique.

Avec le Cachet Electronique, La Poste se positionne, en France, comme le tiers de confiance dans les échanges de données numériques avec ses offres d'Autorité de validation de signature et d'Autorité d'Horodatage.

Le Gouvernement de Monaco utilise l'horodatage pour la signature des passeports, auprès de Sign Server l'un des premiers serveurs de signature multi-protocoles qui proposent ces services à de grandes administrations et grands comptes à travers plusieurs pays.

5.3 Informations réglementaires sur l'horodatage

A Monaco, dans le titre III intitulé : « De la preuve et de la signature électronique », et plus particulièrement pour les articles 18 et 19, la loi monégasque n°1.383 du 2 août 2011 stipule : « *Une lettre simple relative à la conclusion ou à l'exécution d'un contrat peut être envoyée par courrier électronique. L'apposition de la date d'expédition résulte d'un procédé électronique dont la fiabilité est présumée, jusqu'à preuve contraire, lorsqu'il satisfait à des exigences fixées par ordonnance souveraine* » (Cf. : article 18) et « *Une lettre recommandée relative à la conclusion ou à l'exécution d'un contrat peut être envoyée par courrier électronique à condition que ce courrier soit acheminé par un tiers selon un procédé permettant d'identifier le tiers, de désigner l'expéditeur, de garantir l'identité du destinataire et d'établir si la lettre a été remise ou non au destinataire. Le contenu de cette lettre, au choix de l'expéditeur, peut être imprimé par le tiers sur papier pour être distribué au destinataire ou peut être adressé à celui-ci par voie électronique. Dans ce dernier cas, si le destinataire n'est pas un professionnel, il doit avoir accepté expressément l'envoi par ce moyen ou en avoir accepté l'usage au cours d'échanges antérieurs. Lorsque l'apposition de la date d'expédition ou de réception résulte d'un procédé électronique, la fiabilité de celui-ci est présumée, jusqu'à preuve contraire, s'il satisfait à des exigences fixées par ordonnance souveraine. Un avis de réception peut être adressé à l'expéditeur par voie électronique ou par tout autre dispositif lui permettant de le conserver. Les modalités d'application du présent article sont fixées par ordonnance souveraine* » (Cf. : article 19).

En France, le procédé de l'horodatage électronique est présumé fiable, si ce dernier répond à des normes fixées par le décret en Conseil d'État : le décret n° 2011-434 du 20 avril 2011 s'emploie ainsi à définir les exigences techniques à respecter pour qu'un procédé d'horodatage électronique soit présumé fiable, et à encadrer les procédures de certification des dispositifs et de qualification des prestataires de services d'horodatage électroniques.

Le décret et l'arrêté du 20 avril 2011, ne fixent aucune prescription technique impérative à la charge des fournisseurs : les acteurs demeurent donc libres de concevoir et commercialiser des solutions d'horodatage s'écartant du profil établi par le décret, et les utilisateurs restent à même de choisir des procédés d'horodatage fonctionnant avec les exigences du décret et de l'arrêté.

Le cadrage réglementaire de l'horodatage électronique s'inspire ainsi largement du cadre existant en matière de signature électronique. Il s'appuie également sur des travaux de normalisation répandus au niveau européen.

Pour les pays de l'UE, le règlement européen indique dans la section 6 de l'article 42, alinéa 2 : « *La Commission peut, au moyen d'actes d'exécution, établir les numéros de référence des normes en ce qui concerne l'établissement du lien entre la date et l'heure et les données, et les horloges exactes. L'établissement du lien entre la date et l'heure et les données et les horloges exactes sont présumés satisfaire aux exigences fixées au paragraphe 1 lorsqu'ils respectent ces normes. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2* ».

Précisons également l'existence de différentes normes applicables selon le niveau de protection de l'horodatage souhaité.

Ainsi, le document RFC 3161 définit le protocole d'horodatage TSP (Time-Stamping Protocol).

En adéquation avec le RFC 3161, un horodatage certifié est délivré par un tiers certificateur agissant en tant qu'autorité d'horodatage. Il est utilisé pour prouver l'existence de certaines données avant un instant particulier (exemples contrats, recherches de données, dossiers médicaux…), sans que le détenteur puisse antidater les horodatages. Plusieurs autorités de certification peuvent être utilisées conjointement afin d'accroitre la fiabilité et réduire ainsi la vulnérabilité.

Par ailleurs, la norme ANSI ASC X9.95 pour l'horodatage certifié renforce le RFC 3161. Elle permet de certifier les données signées électroniquement, par exemple dans le cadre de transactions financières, de preuves légales…

5.4 Applications : cas concret selon l'exemple du contrat

La loi monégasque n° 1.383 du 2 août 2011 définit le contrat à distance comme suit : « *Tout contrat conclu dans le cadre d'un système de vente ou de prestations de services organisé par le fournisseur qui, pour ce contrat, met en œuvre une ou plusieurs techniques de communication à distance utilisant des moyens électroniques, jusqu'à la conclusion du contrat, y compris la conclusion du contrat elle-même.* »

Cas concret :

La société d'informatique X basée à Monaco vient de vendre du matériel informatique à la société Y établie à Paris.

La procédure à suivre serait la suivante :

→ La société monégasque transmet le contrat de vente par voie électronique en se connectant à un ou des site(s) agréé(s) en matière de signature électronique et d'horodatage.

Monaco

Tiers de confiance

Paris

→ La société parisienne retourne, dûment signé et horodaté, l'ensemble des éléments constituant le contrat de vente préalablement encapsulé électroniquement pour un envoi de type lettre recommandée au format électronique, en se connectant à tout site agréé à sa convenance.

6 ARCHIVAGE ELECTRONIQUE

6.1 Définition

Problématique : conservation sécurisée des données numériques

« La conservation de données numériques » ou « L'archivage de contenus électroniques » est l'ensemble des actions, outils et méthodes mis en œuvre pour réunir, identifier, sélectionner, classer et conserver des contenus électroniques, sur un support sécurisé, dans le but de les exploiter et de les rendre accessibles dans le temps, que ce soit à titre de preuve (en cas d'obligations légales notamment ou de litiges) ou à titre informatif.

Cette conservation numérique s'inscrit dans une démarche globale d'archivage d'une organisation visant, quel que soit le support, papier ou numérique, à assurer une gestion efficace de son information et de ses documents tout au long de leur cycle de vie.

On distingue :

- l'archivage numérique qui répond généralement à une obligation légale et prévoit la traçabilité, la non modification du document et souvent une valeur probante, donc une sécurité accrue,

- la GED qui permet la mise à disposition auprès d'un grand nombre d'utilisateurs des documents pour les partager et a plutôt à vocation interne.

On parlera de conservation sécurisée lorsque l'ensemble des modalités de conservation et de gestion des données permet au support numérique de servir de preuve juridique.

Pour une archive informatique de longue durée, il conviendra de s'assurer de l'indépendance de l'information par rapport à son format : par exemple pour des données archivées pour 20 ans, il est préférable de stocker l'information sous forme de texte brut (.txt ou mieux PDF/A), plutôt que dans un format natif pour lequel le programme associé risque de ne plus être disponible, ou dont le système d'exploitation ne sera plus opérationnel.

La fin de la notion d'archivage électronique (JM Rietsch)

L'archivage des documents a d'abord été organisé et encadré juridiquement autour principalement du papier, en distinguant ses trois âges : courant, intermédiaire et définitif. Est ensuite arrivé l'archivage électronique à la fin du siècle dernier. Pendant presque dix ans l'évolution de l'archivage électronique s'est faite en parallèle à l'archivage papier, avant que l'on assiste finalement à une forme de réconciliation du numérique avec le papier permettant à l'utilisateur d'accéder aux documents archivés d'une seule voie, qu'il s'agisse de documents papiers ou numériques.

Les Anglo-Saxons défendent plutôt la notion de records management, mieux adaptée à l'électronique et surtout qui prend en compte la logique d'archivage très en amont. Existent également d'autres notions comme la GED (Gestion Electronique de Documents) destinée à l'origine à mettre à disposition des utilisateurs des documents numérisés, l'archivage à valeur probante, l'archivage sécurisé, l'archivage légal, l'archivage technique, …

De plus, pourquoi limiter les exigences liées à la valeur probante aux seules données/documents sur lesquels pèsent des obligations légales et réglementaires ? En effet, les exigences en matière de garantie d'origine et d'intégrité sont les mêmes pour toute donnée/document conservé pour peu que leur usage le justifie, en particulier les données historiques ou patrimoniales. Que faire d'un document interrogé au bout de plusieurs années si l'on est incapable de garantir qu'il n'a pas été modifié ?

Mais revenons à l'utilisateur et précisons que l'archivage électronique fait aujourd'hui partie intégrante du système d'information et n'est pas à traiter à part. On assiste en effet à la fin de la rupture existant dans le monde papier, au moment de l'archivage, qui malgré une belle organisation théorique est déclenché souvent à cause d'un manque de place. Il nous faut désormais raisonner sur le cycle de vie des données/documents et prendre en compte la notion de durée de conservation des documents dès leur origine.

Notre besoin, en tant qu'utilisateur, consiste à trouver la bonne information au bon moment à travers le SI et peu importe que les données/documents y soient conservés depuis quelques minutes, plusieurs mois ou plusieurs années. On peut ici se permettre un parallèle avec le Cloud où peu importe l'endroit où se trouve physiquement les données/documents, l'objectif est finalement d'y accéder lorsque l'on en a besoin.

Un tel raisonnement a le mérite de simplifier considérablement le discours vis-à-vis de l'utilisateur mais implique de conserver avec la sécurité adaptée les données/documents en ajoutant la notion de pérennité aux critères sécuritaires classiques (Disponibilité, Intégrité, Confidentialité, Preuve).

La véritable difficulté consiste néanmoins à gérer la transition avec le monde papier pour lequel l'archivage vient après. Il y a donc lieu de repenser le SI de telle sorte que l'information soit conservée une seule fois dans les conditions de sécurité optimum.

Cependant pour des raisons économiques et sécuritaires il peut s'avérer pertinent de gérer par exemple en parallèle un système de type GED, destiné aux accès multiples et rapides avec un autre système plus sécurisé respectant les exigences de l'archivage.

Dans le cadre du projet de conservation numérique sécurisée, à l'issue de la numérisation des documents et sous réserve d'effectuer le traitement dans des conditions de sécurité propres à garantir la fidélité de l'élément numérique résultant, l'organisation pourra détruire les originaux papiers.

Dans ce cas, l'organisation devra s'assurer de la traçabilité dudit document et fera appel à un prestataire agréé par les autorités ou tiers de confiance (valable également pour la signature, l'horodatage et l'AGP) et veillera à choisir une solution d'archivage fiable et pérenne.

Ouverture au big data

Au-delà des gains d'efficacité que procure la conservation numérique sécurisée, l'organisation construit une base informationnelle structurée très pertinente qui permet la valorisation de cette

information et sa transforme en connaissance. On peut l'associer à la démarche « big data » ou comment tirer des informations pertinentes pour accélérer mon business ou la bonne compréhension de certains phénomènes.

De ce qui précède découle naturellement un besoin sans cesse grandissant en solutions de stockage.

Il est aujourd'hui concevable de mettre à disposition de l'entreprise une solution de stockage répondant, à court ou moyen terme, à son besoin. Il faudra dans ce cas privilégier des solutions à base de SAN ou NAS, autorisant une extension des besoins en stockage sans remise en question de l'infrastructure.

Toutefois la conservation numérique de l'intégralité des documents reçus et produits par l'entreprise dépassera rapidement les capacités de stockage interne et demandera d'externaliser la prestation.

De même les traitements nécessaires pour croiser les informations imposeront rapidement l'utilisation de capacités de calcul de plus en plus fortes. A défaut de pouvoir, sans cesse, augmenter les capacités de traitement dans l'entreprise, c'est tout naturellement que celle-ci se dirigera vers une solution de stockage et de traitement déportés.

La conservation des données numériques et le cloud (JM Rietsch)

L'évolution de la technologie a souvent montré une confusion entre besoins, moyens et usages. Les questions soulevées par l'augmentation constante des volumes d'information à gérer en sont la parfaite illustration. En effet, le problème ne se situe pas uniquement au niveau de la gestion du volume final mais également sur la façon de diminuer ce volume dès l'origine. L'e-mail constitue un exemple représentatif de cette situation où tout le monde se plaint des volumes résultants sans pour autant se poser la bonne question de savoir si l'e-mail est bien géré et surtout bien utilisé par rapport à sa fonction d'origine : « l'échange de messages ».

A notre décharge, pratiquement personne n'a véritablement été formé voir simplement informé quant à la façon d'utiliser l'e-mail. Nous roulons ainsi quotidiennement sans code de la route et l'on s'étonne des conséquences, bien évidemment désastreuses en matière de volumétrie avec le contenu de certains e-mails qui peut être conservé plusieurs dizaines voire centaines de fois à l'identique entre multiples destinataires, sauvegardes serveur, fichier historique lui-même sauvegardé. A cela s'ajoutent les spams qui représentent près de 90% des e-mails transmis. Enfin il ne faut pas oublier les conséquences au niveau de la sécurité à prendre au sens large et en particulier concernant la confidentialité des échanges et le respect des règles élémentaires en matière de données personnelles.

L'histoire assez récente de l'informatique, révèle ainsi le paradoxe étrange d'une science, a priori précise, basée sur des choses simples, des « 0 » et des « 1 » mais qui s'est toujours développée dans la plus grande anarchie, poussée par des exigences tant techniques qu'économiques, véritable fuite en avant à la puissance tant des traitements que des volumes de données à gérer en oubliant la plus élémentaire sagesse consistant à prendre un peu de recul de temps en temps afin de vérifier l'adéquation des besoins et des outils !

Face à l'augmentation des volumes, la principale réponse à ce jour consiste à accroître les capacités de stockage en tentant néanmoins de réduire la volumétrie par la mise en œuvre de systèmes de déduplication. Malheureusement les volumes continuent d'augmenter sans cesse et se pose alors un problème de coût, surtout à l'époque actuelle. Curieusement la question de savoir s'il est utile de tout

conserver se pose rarement ou se voit vite abandonnée de par l'ampleur de la tâche et le refus de se lancer dans des opérations de tri périlleuses et somme toute délicates a posteriori et ce d'autant plus qu'elles ne peuvent se faire par un seul service.

Confronté à la difficulté de devoir satisfaire des besoins en volumétrie énorme à des coûts acceptables, on a donc naturellement mutualisé les infrastructures et on s'est alors orienté vers des systèmes externalisés (rendus possible grâce aux nouvelles capacités offertes par les télécommunications), apparus tout d'abord sous la forme d'ASP (Application Service Provider) avant de se transformer en IaaS (infrastructure as a service), premier aspect du cloud computing.

D'un point de vue technique, il est également apparu intéressant d'envisager jusqu'à la mutualisation de plates-formes complètes destinées à offrir un véritable environnement de travail, à la fois hardware et software, d'où la notion de PaaS (Platform as a Service) en particulier pour le développement de nouvelles applications, deuxième aspect du cloud. Cette démarche s'est poursuivie pour finalement aboutir au troisième aspect du cloud, le SaaS (Software as a Service) qui concerne directement l'utilisateur final et lui permet ainsi d'avoir accès aux fonctions dont il a besoins quel que soit l'endroit où il se trouve et à partir d'une multitude de terminaux, sous réserve toutefois de pouvoir accéder au réseau. Ce troisième aspect montre qu'à ce stade, on a largement dépassé la seule vision technique des choses. La logique du SaaS est d'ailleurs plus à prendre comme un modèle économique qui consiste à payer à l'usage en fonction du service demandé.

Le cloud apparaît ainsi comme un moyen de distribuer l'énergie numérique, l'énergie IT tant technique que fonctionnelle qui permet à l'utilisateur de s'affranchir des contraintes liées aux infrastructures informatiques traditionnelles et correspond finalement à l'aboutissement du « nuage internet », du grid computing, du grid storage avec une pointe de virtualisation. Rappelons également que par construction, le cloud peut être aussi bien privé au sein d'une même organisation ou public, partagé entre plusieurs.

A ce jour, les avantages du cloud sont indéniables comme celui de disposer sans contrainte, d'une plate-forme technique équipée avec les dernières technologies ou encore d'accéder à des fonctionnalités de n'importe où en ne payant que leur usage effectif. Mais face à ces avantages, le cloud présente également son lot d'inconvénients dont le principal se situe au niveau de la sécurité au sens global, à la fois technique, juridique et environnementale.

Pour y répondre, il est cependant totalement utopique de chercher à sécuriser le cloud au regard des faiblesses d'ores et déjà identifiées, en s'appuyant uniquement sur des moyens traditionnels. En effet, si l'on prend la sécurité légale et réglementaire, il est bien évidemment très difficile de trouver une véritable réponse en ce qui concerne en particulier la responsabilité du service, à qui incombe-t-elle en cas de problème constaté dans un environnement SaaS vu la multiplicité des acteurs concernés ? Au-delà de cette interrogation se pose également la question de savoir si le droit applicable pour certains types de données est compatible avec une architecture cloud transfrontalière, impliquant des lois et réglementations, parfois contradictoires en fonction des pays concernés.

En complément à la sécurité, n'oublions pas que la confiance constitue le seul véritable moyen de travailler efficacement dans un environnement numérique. En ce sens, l'authentification des personnes et des systèmes revêt un rôle prépondérant et la notion d'identité numérique doit même s'étendre aux documents eux-mêmes.

En effet en tant qu'utilisateur, notre besoin d'aujourd'hui et de demain consiste à trouver la bonne information au bon moment à partir du système d'information auquel on accède, peu importe que les données/documents y soient conservés depuis quelques minutes, plusieurs mois ou plusieurs années et peu importe également l'endroit où se trouve physiquement les données/documents, l'objectif est

bien d'y accéder lorsque l'on en a besoin. Par contre, une fois retrouvé, il est également indispensable de pouvoir avoir confiance dans ce document numérique, en particulier au regard de son origine et de sa non altération, rôle dévolu à son identité numérique.

De ce qui précède découle également le fait de devoir se pencher sur l'organisation de l'information afin de pouvoir la retrouver facilement. Si aujourd'hui la question du tri de l'information est trop souvent éludée, il est cependant important de s'y arrêter et d'agir dès à présent en amont afin de disposer d'une information bien organisée, facilitant l'ensemble de ses traitements et en particulier ses accès, sa conservation et sa suppression. Le maître mot est ici de prévenir plutôt que de guérir.

Ainsi n'en sommes-nous qu'au début de la logique de cloud qui allie organisation technique et modèle économique et dont la prochaine étape consistera vraisemblablement en la naissance de ce que l'on peut d'ores et déjà qualifier de « centrales numériques » délivrant de l'énergie IT. Le cloud permet déjà, et sous réserve des contraintes exposées, de respecter le triangle vertueux du système d'information, les 3 « V » : volume, vitesse (traitements et transferts) et valeur. Cette dernière joue un rôle essentiel et justifie pleinement la mise en place de la sécurité nécessaire et surtout adaptée au type de données/documents visés. En effet, la valeur de l'information et plus encore sa valorisation ne constituent-ils pas la base de notre patrimoine informationnel, autre vaste sujet.

Les supports de demain pour la conservation des données numériques

Rappelons tout d'abord qu'au niveau logique, la conservation des données numériques tant sur le long terme que sur le court ou moyen terme passe obligatoirement par une bonne organisation des informations et la présence de données complémentaires, les métadonnées, véritables identité numérique des documents permettant de les retrouver facilement et efficacement. D'un point de vue plus physique et matériel, le besoin correspond bien sûr à disposer de systèmes offrant des capacités de stockage de plus en plus en plus importantes. De plus pour le moyen et surtout le long terme la tentation est grande de chercher des technologies avec des supports les plus pérennes possibles. Or sur ce dernier point il est clair que le dispositif idéal n'existe pas encore, quoique ! Mais surtout devra-t-on avant toute chose s'attacher à choisir un format logique pérenne, destiné à garantir l'intelligibilité des données dans le temps. Il s'agit là d'un sujet particulièrement sensible pour lequel beaucoup reste encore à faire.

Du côté matériel, les sceptiques vis-à-vis du numérique nous rappellent qu'il est encore possible aujourd'hui de lire des informations gravées dans la pierre, pour ne pas dire sur le marbre ! Certes, mais il n'en est pas moins vrai que plusieurs pierres, identiques à la pierre de Rosette ont été retrouvées mais se sont révélées totalement inexploitables dans la mesure où les caractères gravés avaient été pratiquement totalement effacés par le sable. Ainsi, quel que soit le support, la façon dont il est lui-même conservé est également essentielle, le CD en est également la parfaite illustration et qui n'a pas eu un jour la désagréable surprise de ne plus parvenir à lire un CD conservé sans précaution particulière ?

Retour à la pierre !
Et si demain l'on revenait à la pierre, plus précisément au quartz, pour permettre le stockage de données numériques sur un matériau finalement aussi peu coûteux et basique que le verre ? Cette réalité n'est peut-être pas aussi loin qu'il y paraît dans la mesure où Hitachi a présenté récemment un prototype sous la forme d'un simple morceau de quartz rectangulaire, d'une surface de deux centimètres carrés et d'une épaisseur de deux millimètres. Très résistant, sauf aux chocs, il serait capable d'endurer une exposition directe aux flammes, à une température de 1.000 degrés Celsius, pendant deux heures avant d'être compromis. Il résisterait également aux ondes radio, aux produits chimiques, et aux liquides. La densité de stockage serait comparable aux CD, grâce à quatre couches de gravure. Il ne devrait pas y avoir de problème pour ajouter des couches supplémentaires, et

accroître ainsi la densité de stockage. Le prototype présenté peut stocker environ 6,2 Mo par centimètre carré de surface soit 40 Mo par pouce carré contre 35 pour un CD.

En dehors de la durée de stockage, le prototype ainsi présenté résoudrait également le problème de la lisibilité des données dans le temps dans la mesure où les informations conservées sur le support de quartz seraient lisibles avec un simple microscope optique. Donc quelle que soit la technologie de lecture utilisée, un ordinateur sera capable de récupérer les données stockées en binaire. Restera cependant à les interpréter, rôle dévolu au format logique employé, comme vu précédemment.

Qu'attendre des nouvelles technologies optiques ?
Plus proche de nous, la mémoire holographique a permis de gros progrès en matière de densité de stockage et de taux de transferts. Contrairement aux autres méthodes qui stockent les données en deux dimensions sur les couches d'un média, les données holographiques sont stockées de façon volumétrique, dans l'épaisseur même du média, en trois dimensions. Par ailleurs les données sont stockées et lues dans un format de page contenant environ 60.000 bits là où dans le même temps un DVD en retrouve 1 ! Dans son principe général et théorique, la mémoire holographique consiste à stocker les données par des méthodes optiques dans des cristaux photosensibles.

A ce jour, le HVD pour Holographic versatile disc est une technologie de disque optique qui peut contenir jusqu'à 3,9 To d'information soit 5.800 CDs ou 830 DVD ou encore 60 Blu-ray. La plus grande bibliothèque au monde, celle du congrès américain, tiendrait ainsi sur six HVDs ! Les taux de transfert sont de 1 Gbit/s contre 36 Mbit/s pour un Blu-ray et seulement 11 Mbit/s pour un DVD. Le HVD est ainsi amené à remplacer les DVDs et est déjà supporté par plus de 170 des leaders mondiaux en matière électronique.

Les évolutions au niveau des systèmes magnétiques
Mais qu'en est-il des dispositifs basés sur le magnétique ? En fait trois grandes familles sont à prendre en compte, les disques, les mémoires flash et les bandes. Pour l'ensemble, les progrès en matière de densité de stockage sont constants, sans doute un peu plus rapide pour les bandes comme le laisse entrevoir un rapport IBM qui prévoit qu'entre 2010 et 2014, les bandes passeront d'une densité de 1,2 Gbit par pouce carré à 4,8 Gbit. Dans le même temps pour les disques magnétiques on passerait de 635 Gbit par pouce carré à 2.500 soit 2,5 Tbit et pour les mémoires flash de 330 Gbit par pouce carré à 1.300.

De façon concrète, dès 2012 Seagate a atteint une densité de stockage de 1 Tbit par pouce carré en utilisant une technologie très prometteuse nommée HAMR (Heat-Assisted Magnetic Recording) qui pourrait donner naissance à des disques de 3,5 pouces offrant jusqu'à 60 téraoctets de capacité de stockage d'ici 10 ans.

Plus récemment, le constructeur HGST, filiale de Western Digital, vient d'annoncer la mise au point d'une autre nouvelle méthode de stockage des données qui permettrait à terme de doubler la densité de stockage de nos disques durs. Basée sur l'utilisation de la nanolithographie et de molécules capables de s'auto-assembler, cette méthode serait capable de générer un masque « répétitif » à base de polymères hybrides permettant ensuite de créer des ilots magnétiques de seulement 10 nm (soit 50 atomes de large), chacun étant capable de stocker un bit. Cette technique permet ainsi d'atteindre 1.200 milliards de bits (1,2 Tbit) par pouce carré, soit une densité deux fois plus importante que les disques durs actuels.

Cette quantité de 50 atomes de large corrobore l'annonce faite début 2012 par les chercheurs de chez IBM qui expliquaient avoir réussi à stocker un bit de donnée magnétique dans seulement 12 atomes mais à -272,15 °C. Ces mêmes chercheurs prévoyaient alors que pour fonctionner à température ambiante, il faudrait environ 150 atomes pour stocker un bit de donnée magnétique.

Enfin une nouvelle mémoire magnétique haute densité a été récemment annoncée. Une équipe de chercheurs a en effet montré une méthode permettant de produire une cellule de mémoire magnétique organique utilisant du cobalt, ainsi qu'un métal organique répondant au nom de zinc-méthyle-phénalényle (ZMP).

Preuve que le stockage magnétique est encore loin d'avoir révélé ses limites.

Et si la révolution venait du vivant !
Nous terminerons par une annonce de janvier 2013 particulièrement prometteuse en matière de stockage d'information sur de l'ADN. Des chercheurs de l'European Bioinformatics Institute (EBI – Royaume Uni) ont en effet réussi à stocker 6 mégabits, dans 337 picogrammes d'ADN ! Après la cassette, les disquettes, les disques, les CD, les clés USB et les mémoires flash, la molécule où sont inscrits nos gènes pourrait-elle devenir LE support de stockage par excellence ? L'ADN présente en effet de grands avantages et en particulier il peut contenir beaucoup d'informations avec une densité très importante, les chercheurs annoncent 2 petaoctets dans un seul gramme !

Reste à produire dans des conditions économiques acceptables mais gageons que les dix prochaines années verront sans doute le développement effectif des nouvelles technologies telles qu'elles viennent d'être exposées, d'autant plus que certaines sont déjà largement avancées sur le sujet.

6.2 Importance d'une méthodologie

6.2.1 La politique d'archivage (PA) comme élément de gouvernance

Dans la démarche de conservation, le contenu archivé est considéré comme figé et ne peut donc être modifié. La durée de la conservation est fonction de la valeur du contenu et porte le plus souvent sur du moyen ou long terme. Ainsi une organisation mettra en place sa politique de conservation numérique en :

- choisissant les documents à archiver :
  - pourquoi conserver ce document ?
  - est-il obligatoire de le conserver ?
  - pour quelle durée ?

- identifiant les différents intervenants (versant, contrôleur, usager), leurs rôles et responsabilités,

- décrivant les processus à mettre en œuvre :
  - comment conserver les documents ?
  - comment y accéder ?

- définissant les niveaux de sécurité en matière de disponibilité, intégrité, confidentialité, traçabilité.

De l'archivage électronique à la gouvernance de l'information (JM Rietsch)

Les enjeux liés à la problématique de l'archivage électronique sont encore loin d'être appréhendés à leur juste dimension, alors même qu'il s'agit d'une partie intrinsèque du système d'information de toute organisation. Les incompréhensions font légion dont les origines sont à chercher tant du côté de la fausse image que l'on a généralement de l'archivage que d'une volonté de vouloir à tout prix définir, différencier voire plus grave opposer la GED, l'archivage ou encore le records management. En réalité, les objectifs de base sont identiques et consistent à suivre/tracer, collecter, conserver et retrouver cette précieuse information que l'on a de plus en plus de mal à maîtriser. Là encore la principale difficulté, contrairement à ce que l'on a tendance à penser, ne provient pas des volumes mais principalement de la qualité et de la sécurité de l'information.

Par ailleurs, le fait d'être passé ces dernières années de la gestion de la sécurité à la gestion du risque constitue une évolution radicale du système d'information et l'obligation de devoir répondre au paradoxe consistant à gérer des accès de plus en plus nombreux pour des utilisateurs aux profils très variés, tout en assurant un niveau de sécurité indispensable. Le défi à relever est loin d'être simple, néanmoins c'est bien de cela dont il s'agit et les responsables chargés de cette gestion sont de véritable orfèvres quant à la façon d'identifier les risques, les quantifier et les classifier afin de pouvoir mettre en place des solutions sécuritaires efficaces et adaptées sachant par principe qu'elles ne répondront pas à l'intégralité des risques relevés, d'où cette notion de risque résiduel de plus en plus développée. En matière d'archivage cela peut se traduire par la réponse à donner à la simple question : sommes-nous prêt à perdre telle ou telle information ?

L'archivage électronique s'inscrit donc parfaitement dans cette démarche. En effet, sachant que par principe, toutes les données au sein d'une organisation n'ont pas la même valeur, il n'y a aucune raison pour les gérer et surtout les archiver de la même façon, avec les mêmes risques, sachant que les solutions proposées n'ont évidemment pas les mêmes coûts en fonction du niveau de sécurité requis et du niveau de performance désiré. Même si bien évidemment « qui peut le plus, peut le moins » pourquoi dépenser plus si cela n'est pas vraiment nécessaire, surtout en période d'austérité. Là encore, le responsable de cette gestion devra faire preuve de talent pour trouver un juste milieu entre la complexité du découpage à effectuer quant aux différentes infrastructures et à l'organisation à mettre en œuvre par rapport aux gains à attendre en retour. Pour cela il dispose néanmoins d'outils précieux en particulier au travers des politiques de sécurité et des politiques d'archivage.

La démarche précédente ne doit pas se limiter à l'archivage électronique mais au contraire doit bien s'étendre à l'ensemble du système d'information qui se retrouve au cœur de ces préoccupations, en tant que support de l'ensemble des processus métier de toute organisation. Par ailleurs et comme vu précédemment, il doit s'ouvrir à un nombre d'utilisateurs de plus en plus grand, répondre à une augmentation des capacités de stockage et de traitement mais surtout passer d'une logique de simple collecte des données à une véritable logique de production d'informations et de création de valeur. En ce sens, le système d'information participe de plus en plus au patrimoine informationnel des organisations, véritable actif immatériel.

Néanmoins toutes ces évolutions ne peuvent se faire de façon efficace que si l'on se dote d'instruments de référence et d'une organisation appropriée du système d'information constituant ainsi une véritable gouvernance de l'information. Cette dernière doit ainsi permettre au système d'information de reposer sur des bases solides et des principes connus de tous les acteurs, en particulier en dotant l'organisation d'outils de référence : documents stratégiques, moyens de communication et d'organisation, systèmes de conservation et d'archivage. Sur ce dernier point nous pourrions même oublier un instant le terme « archivage » et parler simplement de conservation à plus ou moins long termes !

En élaborant sa politique de gestion de son information et en documentant ses processus métier, toute organisation s'inscrit dans une démarche de responsabilité économique, sociale et juridique vis-à-vis des autorités extérieures, de ses clients, de ses fournisseurs et de ses collaborateurs. La politique documentaire et d'archivage pose en fait les bases de sa politique en matière de gestion de l'information, de son information et des engagements qu'elle prend en matière de gouvernance. En effet, cette politique de l'information et les procédures et documents liés à chaque processus métier sont la garantie de la mise en place cohérente de l'activité en conformité avec les exigences internes, légales, réglementaires ou normatives qui s'imposent à toute organisation en regard des besoins de sécurité et de ses besoins métier.

Par ailleurs chacun des départements à l'intérieur de l'organisation possède ses propres exigences, ses propres contraintes légales et réglementaires qu'il soit financier, informatique, juridique avec en particulier la gestion des données personnelles…Chacun d'eux se doit ainsi d'être organisé avec ses propres politiques, tenant compte bien évidemment des politiques globales de l'organisation et des contrôles permettant de régir l'information tout en prévoyant également les processus nécessaires à appliquer en cas d'incidents.

La gouvernance de l'information touche en fait beaucoup de domaines importants déjà largement évoqués, comme la classification des données, la qualité de l'information (pouvoir répondre à la question : puis-je faire confiance à cette information ?), l'élaboration des différentes politiques, la gestion du cycle de vie de l'information (ILM pour information life cycle management), la gestion du risque et de la conformité (GRC gouvernance, risk & compliance) sans omettre l'un des domaines les plus cruciaux et stratégique représenté par la valorisation de l'information.

Retenons que la gouvernance de l'information, au-delà des mots, constitue un moyen extrêmement important permettant de transformer l'information, de la valoriser, d'atteindre la connaissance. Comme évoqué précédemment, seule une prise en compte globale de l'ensemble des domaines identifiés à l'intérieur de la gouvernance de l'information permettra d'obtenir des résultats tangibles. Prendre conscience que l'informatique n'est pas plus importante qu'un service juridique ou tout autre service et réciproquement, est fondamental. La vérité n'appartient ni à l'un ni à l'autre et il s'agit pour toute organisation de relever le défis d'ordonner tous les domaines concernés en un ensemble cohérent de politiques et de contrôles valables à travers tous les systèmes, les fonctions et les implantations géographiques de l'organisation.

Face à l'augmentation des volumes de données et des échanges, il est de plus en plus essentiel d'organiser l'information, l'immatériel de toute organisation et prendre conscience de l'importance de la mise en place d'une véritable gouvernance de l'information, destinée à la fois à protéger mais surtout à valoriser ce véritable patrimoine informationnel. Des lieux communs comme « trop d'information tue l'information » n'ont pas lieu d'être à partir du moment où l'information est bien gérée, bien gouvernée. Une telle affirmation correspond plutôt à un véritable aveux d'impuissance à organiser l'information de façon fiable et efficace permettant à l'utilisateur de retrouver la bonne information au bon moment et en toute confiance, que l'information ait quelques minutes d'existence, quelques mois ou plusieurs années.

Tant la dématique que l'archivage électronique sont directement concernés par ce véritable défi lié à la gouvernance de l'information, comme partie intégrante du système d'information. De fait, de tels projets doivent ainsi relever directement de la direction générale de toute organisation et être traités de façon transverse, ils ne doivent plus être abordés comme de simples « gadgets » techniques, de manière isolée et souvent incomplète par rapport à un besoin mal exprimé voire pas exprimé du tout et surtout ne plus être renvoyés d'un service à un autre sous prétexte que l'on ne se sent pas concerné où que l'on ne dispose pas des compétences nécessaires. Apprenons plutôt à travailler ensemble et soyons d'autant plus efficace.

Le défi est d'importance, car lui seul permettra à toute organisation de profiter de cette véritable richesse que constitue l'information à partir du moment où elle est correctement gérée et surtout exploitable et transformée en connaissance. N'oublions pas également que valorisation de l'information peut aussi vouloir signifier innovation et par voie de conséquence compétitivité !

6.2.2 L'analyse du risque

Pour correctement orienter notre travail, il faudrait dès le début introduire une notion de risque. Cette notion consisterait à établir différents niveaux autour du principe DICP.

Nous définissons d'abord les DICP (1.) pour pouvoir ensuite définir les niveaux de service (2.)

1. Le DICP :

- Disponibilité
- Intégrité
- Confidentialité
- Preuve-trace-auditabilité

La sécurité informatique consiste à garantir que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu.

(Réf : JF Pillou, Tout sur les systèmes d'information, Paris Dunod 2006, Collect° Commentcamarche.net)

Plusieurs types d'enjeux doivent donc être maitrisés.

Derrière cette abréviation se cachent les objectifs de la Sécurité des Systèmes d'Information (SSI) qui peuvent se traduire en termes d'exigences de :

- Disponibilité :
Propriété d'accessibilité des éléments essentiels au moment voulu par les utilisateurs autorisés. Cette propriété peut aussi être exprimée sous la forme d'un niveau de service attendu dans un contrat de service (SLA pour service level agreement). Cela peut correspondre à la durée nécessaire pour avoir accès au bien essentiel (ex. : 1 heure, 1 journée, 1 semaine…).

- Intégrité :
Propriété d'exactitude et de complétude des éléments essentiels. Cela correspond autant à leur niveau de conformité qu'à leur stabilité, leur exactitude, leur complétude.

- Confidentialité :
Propriété des éléments essentiels de n'être accessible qu'aux utilisateurs autorisés (préservation des données sensibles). Cela correspond au nombre ou catégories de personnes autorisées à y accéder.

- Preuve :
Garantie de ne pas pouvoir réfuter l'émission ou la réception d'une information, avec possibilité de pouvoir auditer les résultats fournis (exemple : un virement de fonds et la vérification du journal comptable à partir des informations d'entrée).

(Réf. : EBIOS v2 – Section 3 – Techniques – 5 février 2004)

Ces quatre points sont des critères de sécurité représentant des fondamentaux notamment pour assurer la continuité de la communication et de la diffusion des informations confidentielles.

Suivant l'importance d'une information selon chaque critère, des mesures différentes pour en assurer la sécurité vont être mises en place.

Dans le domaine de la sécurité du système d'information, on classe systématiquement les informations suivant ces critères, ce qui déterminera comment elles doivent être gérées.

Il faut choisir quels critères sont les plus importants, en fonction des besoins des utilisateurs.

En pratique, en se donnant une échelle quantitative pour les différents critères (niveaux), on va pouvoir construire un système d'information avec une gradation de solutions adaptées suivant les besoins, avec évidemment des mesures d'autant plus coûteuses que :

- L'importance pour tel ou tel critère est élevée : plus elle est élevé, plus les coûts le sont aussi (avoir besoin de l'information dans la seconde est plus coûteux que dans la journée, en avoir besoin uniquement à un endroit n'a rien à voir à en avoir besoin dans le monde entier…)

- Les besoins sont élevés pour plusieurs critères simultanément : dans ce cas les solutions peuvent être complexes et très coûteuses. On peut citer l'exemple des solutions de réservations aériennes, qui exigent une disponibilité en temps réel et au niveau mondial, une fiabilité (intégrité) à tout épreuve, la confidentialité des données personnelles, ainsi que la traçabilité et preuve des transactions : d'où le coût très élevé des solutions en question.

(Réf : http://securid.novaclic.com)

6.3 Niveaux de service : déterminer l'échelle de besoins

Les besoins de sécurité devront s'exprimer pour chaque critère de sécurité sélectionné. Une graduation des besoins de sécurité doit être élaborée sous la forme de niveaux de besoins. Pour cela, une définition doit être formulée pour chaque niveau de besoins de chaque critère de sécurité.

Il est néanmoins envisageable de définir une échelle comprenant un nombre de niveaux différent.
Il est préférable que le nombre de niveaux soit le même pour chaque critère de sécurité.
Dans la mesure du possible, les valeurs de références doivent être explicites et comprendre un ensemble de valeurs bornées. Nous donnons ci-après à titre indicatif des exemples de valeurs pour les critères sécuritaires.

6.3.1 Disponibilité :

Durée maximum d'indisponibilité	Note
Aucune contrainte	1
1 semaine	2
2 jours	3
4 heures	4

6.3.2 Intégrité :

Besoins client	Note
Pas de besoin particuliers en matière d'intégrité	1
Perte d'intégrité tolérée mais doit être détectée et signalée	2
Perte d'intégrité tolérée mais doit être détectée et corrigée	3
Aucune perte d'intégrité tolérée	4

6.3.3 Confidentialité :

Type de confidentialité	Note	Commentaire
Données publiques	1	Ces informations sont destinées à être largement diffusées Elles ne font l'objet d'aucune protection de confidentialité particulière.
Données à diffusion restreintes	2	La divulgation de telles informations est susceptible d'entraîner des préjudices pour l'organisme propriétaire des données, sans le mettre directement en péril.
Données confidentielles	3	La divulgation de ces informations peut entraîner des préjudices graves pour l'organisme propriétaire. Ces informations sont soumises à des règles de protection particulièrement rigoureuses.
Données très confidentielles	4	La divulgation de cette information pourrait causer un dommage exceptionnellement grave allant jusqu'à la disparition de l'organisme dont elle émane.

6.3.4 Preuve-Traces :

Les traces doivent être opposables et restituables. Il n'y aura pas de trace des accès en interrogation pour les documents librement communicables.

Note	Besoins client/cycle de vie des données/documents
1	Action système technique et fonctionnel
2	Qui, quand (horodatage), quelle action, sur quoi (suppression/modification/création)

3	Qui, quand (horodatage), quelle action, sur quoi (suppression/modification/création/Accès)
4	Qui, quand (horodatage), quelle action, sur quoi (suppression/modification/création/Accès), et pour la modification : ancienne valeur, nouvelle valeur

Remarque : Les journaux sont des éléments essentiels qui auront leurs besoins de sécurité spécifiques, notamment en intégrité, qui pourra aller jusqu'à l'enregistrement unitaire et donc des chainages enregistrement par enregistrement.

6.3.5 Niveaux de service

En s'appuyant sur les valeurs précédentes des critères sécuritaires on pourra alors définir les niveaux de service dans un tableau à double entrée comme celui présenté :

Niveaux de service	**Disponibilité**	**Intégrité**	**Confidentialité**	**Trace Preuve**
Niveau 4 de services très fort	4	4	4	4
Niveau 3 de services fort	3	3	3	3
Niveau 2 de services moyen	2	2	2	3
Niveau 1 de services faible	1	1	1	2

Cette échelle doit être adaptée au contexte de l'entreprise avec la participation des personnes qui vont déterminer les besoins. Ainsi, chaque valeur aura une réelle signification pour eux et les valeurs seront cohérentes.

Tous les documents dans l'entreprise n'ont pas la même « importance », la même « criticité » et il n'y a donc aucune raison de les conserver de la même façon, sachant bien évidemment qu'un niveau 4 vaudra beaucoup plus cher qu'un niveau 1.

L'idée à donner aux entreprises est d'optimiser leurs coûts pour investir dans la dématérialisation. Mais généralement elles ne savent pas par où commencer.

En matière de conservation, il est nécessaire de partir sur une base solide représentée par la politique d'archivage qui permet également de poser les bonnes questions comme celle de savoir quelles sont les exigences légales (ou pas) du client et ses besoins ?

7 PREUVE

7.1 Contexte

Le droit civil monégasque était organisé, jusqu'à récemment, exclusivement autour de l'écrit revêtu d'une signature manuscrite. Sous l'influence du droit international et de la législation des pays voisins, la Loi 1.383 sur l'économie numérique en date du 8 août 2011 est venue inaugurer un vrai changement culturel, en consacrant la reconnaissance de l'écrit électronique, à la fois à titre *ad probationem* mais aussi *ad validitatem*, et la signature numérique.

Ainsi, aux côtés des contrats traditionnels, l'échange des consentements peut maintenant s'effectuer dans un environnement numérique, et les contrats numériques peuvent acquérir force probante à l'instar de leurs équivalents physiques.

Ces nouveaux processus de dématérialisation qui forment aujourd'hui notre quotidien, pour simples qu'ils apparaissent, nécessitent cependant une connaissance fine des contraintes légales et une interprétation juridico-technique des moyens à mettre en œuvre, afin d'être fidèles à l'esprit et à la lettre des textes d'autant que les Ordonnances Souveraines devant les expliciter n'ont à ce jour pas été publiées. Il est donc nécessaire d'opérer un rapprochement entre juristes et techniciens.

Il est en effet primordial de définir les exigences juridiques qui s'appliquent à la dématérialisation. Le respect et l'interprétation des dispositions législatives et réglementaires (à venir) conditionneront la validité et l'opposabilité de l'opération dématérialisée.

La mise en place de bonnes pratiques techniques et organisationnelles au meilleur état de l'art ne pourra se faire sans une relecture juridique indispensable lors de chacune des étapes de la dématérialisation : identification, authentification des parties, traçabilité, horodatage, signature électronique, archivage sécurisé ou à valeur probante.

Cette analyse des textes constitue le prérequis indispensable sur lequel s'appuie le choix des outils technologiques à mettre en œuvre. Ainsi, la force de la preuve électronique est subordonnée à la condition de présenter des garanties d'intégrité et de fiabilité des procédés mis en œuvre.

Si l'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, ce n'est que 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.

La garantie de l'intégrité recouvre tant les modalités d'établissement du document, que celles de sa conservation et de sa restitution.

7.2 Conditions légales d'admissibilité en preuve de l'écrit électronique

La loi 1.383 du 2 août 2011 sur l'Economie Numérique reconnait l'écrit électronique en droit monégasque, en lui conférant la même force probante que l'écrit traditionnel.

Le droit de la preuve se traduit par de nouvelles dispositions dans le Code civil et dans le Code de procédure civile.

D'une part, l'article 1163 du Code civil définit la preuve par écrit. Il dispose que « L*a preuve littérale, ou preuve par écrit, résulte d'une suite lisible de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible quels que soient leur support ou leurs modalités de transmission.* ».

Le nouvel article 1163-1 du Code civil pose quant à lui le principe de l'admissibilité en preuve de l'écrit électronique *« au même titre et avec la même force probante que l'écrit sur support papier (…) »*.

On peut donc considérer comme preuve littérale un écrit dématérialisé qui ne dépend plus de la nature de son support ou de sa modalité de transmission.

L'écrit numérique se distingue de l'écrit papier en ce qu'il dissocie l'information (le contenu) et le support (le contenant). D'un point de vue juridique, cette dissociation donne à l'écrit sous forme électronique une apparence de moindre fiabilité par rapport à l'écrit papier.

C'est pourquoi d'autre part, le législateur a posé des conditions pour qu'un écrit numérique soit, en termes de preuve, l'égal d'un écrit traditionnel.

La force probante d'un document électronique est définie à la suite de l'article 1163-1 du Code civil, qui précise les conditions auxquelles doit répondre cet écrit afin d'être utilisé à titre de preuve :

1. la personne (physique ou morale) dont il émane doit pouvoir être dûment identifiée (connaissance de l'origine de l'écrit numérique),

2. il doit avoir été établi et conservé dans des conditions de nature à en garantir l'intégrité (condition rapprochant l'écrit numérique de l'écrit papier, ce dernier la remplissant par essence),

En pratique, la signature électronique est le procédé technique consacré par la loi, permettant d'identifier la personne dont émane l'écrit, et de garantir l'intégrité du document signé.

Comme le précise l'article 1163-3 du code civil : « *La signature nécessaire à la perfection d'un acte juridique identifie son auteur et manifeste son consentement aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte* ».

Elle peut être manuscrite ou électronique.

La signature électronique est une signature qui consiste en l'usage d'un procédé fiable d'identification et garantissant son lien avec l'acte auquel elle s'attache.

Le procédé est présumé fiable, jusqu'à preuve contraire, lorsqu'il garantit l'identité du signataire et l'intégrité de l'acte dans les conditions définies par ordonnance souveraine.

Le législateur a créé une présomption de fiabilité de la signature électronique (la charge de la preuve incombe à l'autre partie). Cependant, les ordonnances souveraines devant fixer les conditions à remplir n'ont, à ce jour, pas encore été publiées.

On ne peut donc pas, en l'état actuel de la réglementation, bénéficier de la présomption de fiabilité du procédé de signature.

Remarque : On peut légitimement se poser la question de savoir s'il est possible d'utiliser une signature électronique qui répondrait aux critères français (utilisation d'un dispositif de création sécurisé de la signature, délivrance d'un certificat qualifié, signature sous le contrôle exclusif du signataire) et, dans une telle hypothèse, sur l'attitude qui serait alors adoptée par le Juge monégasque quant à sa valeur probante (article 279 du Code de procédure civile modifié par la Loi 1.383), sachant que les certificats utilisés à Monaco proviennent eux aussi de France.

A notre connaissance, il n'existe pas encore de jurisprudence sur la question.

Notons enfin qu'en cas de conflit de preuve entre un écrit sous forme électronique (dont la fiabilité du procédé électronique a déjà été vérifiée) et un écrit sur support papier, l'article 1163-2 du Code civil (créé par la Loi 1.383) reprend le principe général gouvernant les conflits entre actes sous seing privé, sans fixer aucune hiérarchie. Le juge doit lever le doute en recherchant le titre qui retrace le mieux la volonté réelle des parties :

« *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.* »

7.3 Actes authentiques électroniques

En principe, un acte authentique implique la présence simultanée des parties, ce qui peut représenter une contrainte.

L'article 1164 du Code civil (modifié par la loi n° 1.383 du 2 août 2011) reconnaît à l'acte authentique électronique, pratique et rapide, la même valeur que l'acte authentique papier, dès lors que les conditions réglementaires à venir seront respectées :

« *L'acte authentique est celui qui a été reçu par officiers publics ayant le droit d'instrumenter dans le lieu où l'acte a été rédigé, et avec les solennités requises.*

L'acte authentique peut être dressé sur support électronique s'il est établi et conservé dans des conditions fixées par ordonnance souveraine. »

Le pays voisin a opté pour l'adoption d'une réglementation par professions (notaires et huissiers de justice).

7.4 Actes sous seing privé électroniques

Il est également possible de conclure électroniquement des actes sous seing privé. Ce point a été abordé par Me Giaccardi lors de sa présentation en date du 17 septembre 2013.

Comme le mentionne Me Giaccardi, la loi n'a pas créé de distinction et un contrat électronique n'aura pas moins de valeur qu'un contrat papier traditionnel.

Pour qu'un acte sous seing privé électronique ait la valeur d'une preuve parfaite de la même façon que l'écrit papier, encore faut-il qu'il réponde à la condition posée par le législateur, à savoir l'utilisation de la signature électronique, conformément aux dispositions des articles 1163-1 et 1163-3 du Code civil.

Réglementation monégasque : Loi n. 1.383 du 02/08/2011 sur l'Économie Numérique

Livre - III DES DIFFÉRENTES MANIÈRES DONT ON ACQUIERT LA PROPRIÉTÉ

(Décrété le 25 octobre 1884 et déclaré exécutoire à dater du 1er janvier 1885)

Titre - III DES CONTRATS OU DES OBLIGATIONS CONVENTIONNELLES EN GÉNÉRAL

Chapitre - VI DE LA PREUVE DES OBLIGATIONS ET DE CELLE DU PAIEMENT

Section - I De la preuve littérale

De l'acte sous seing privé

(Ancien § II dénuméroté par la loi n° 1.383 du 2 août 2011)

Article 1173. - (Remplacé par la loi n° 1.383 du 2 août 2011)

Le billet ou la promesse sous seing privé par lequel une seule partie s'engage envers l'autre à lui payer une somme d'argent ou une chose appréciable doit être écrit en entier par celui qui le souscrit, ou du moins, il faut qu'outre sa signature, il ait écrit par lui-même un bon ou un approuvé, portant en toutes lettres la somme ou la quantité de la chose.

Titre - III DES CONTRATS OU DES OBLIGATIONS CONVENTIONNELLES EN GÉNÉRAL

Chapitre - VI DE LA PREUVE DES OBLIGATIONS ET DE CELLE DU PAIEMENT

Section - I De la preuve littérale

De l'acte sous seing privé

(Ancien § II dénuméroté par la loi n° 1.383 du 2 août 2011)

Article 1172. - (Modifié par la loi n° 1.383 du 2 août 2011)

Les 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 écrits sous forme électronique lorsque l'acte est établi et conservé conformément aux articles 1163-1 et 1163-3 et que le procédé permet à chaque partie de disposer d'un exemplaire ou d'y avoir accès.

Livre - III DES DIFFÉRENTES MANIÈRES DONT ON ACQUIERT LA PROPRIÉTÉ

(Décrété le 25 octobre 1884 et déclaré exécutoire à dater du 1er janvier 1885)

Titre - III DES CONTRATS OU DES OBLIGATIONS CONVENTIONNELLES EN GÉNÉRAL

Chapitre - VI DE LA PREUVE DES OBLIGATIONS ET DE CELLE DU PAIEMENT

Section - I De la preuve littérale

Des dispositions générales (§ créé par la loi n° 1.383 du 2 août 2011)

Article 1163-3. - (Créé par la loi n° 1.383 du 2 août 2011)

La signature nécessaire à la perfection d'un acte juridique identifie son auteur et manifeste son consentement aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte.

Elle peut être manuscrite ou électronique.

La signature électronique est une signature qui consiste en l'usage d'un procédé fiable d'identification et garantissant son lien avec l'acte auquel elle s'attache.

Le procédé est présumé fiable, jusqu'à preuve contraire, lorsqu'il garantit l'identité du signataire et l'intégrité de l'acte dans les conditions définies par ordonnance souveraine.

Notons que la signature électronique ne peut pas néanmoins être utilisée pour « *1° les actes sous seing privé relatifs au droit de la famille et des successions ; 2° les actes sous seing privé relatifs à des sûretés personnelles ou réelles, de nature civile ou commerciale, souscrits par des personnes agissant*

à des fins qui n'entrent pas dans le cadre de leur activité commerciale ou professionnelle » (article 963-2 du Code civil).

Si la Loi du 2 août 2011 consacre la notion d'écrit électronique, elle ne traite pas spécifiquement du cas des échanges d'écrits électroniques, autrement dit des échanges de courriels, pourtant très fréquents en pratique.

L'article 18 de la Loi traite de l'envoi d'un écrit par voie électronique : « une lettre simple relative à la conclusion ou à l'exécution d'un contrat peut être envoyée par courrier électronique.

L'apposition de la date d'expédition résulte d'un procédé électronique dont la fiabilité est présumée, jusqu'à preuve contraire, lorsqu'il satisfait à des exigences fixées par ordonnance souveraine. »

Une fois les conditions réglementaires en vigueur, la signature électronique présumée fiable apposée à un courrier électronique lui donnera force probante parfaite. La conclusion des contrats par voie électronique en sera facilitée.

Les actes sous seing privé qui ne bénéficient pas d'une signature électronique ne sont pas dénués de force probante.

Comme le précise l'article 279 du Code de procédure civile, les écrits électroniques qui ne remplissent pas les conditions des articles précités, à savoir 1163-1 et 1163-3 du Code civil, peuvent toutefois valoir commencement de preuve par écrit, défini par l'article 1194 du Code civil, alinéa 2, comme « *tout acte par écrit qui est émané de celui contre lequel la demande est formée ou de celui qu'il représente, et qui rend vraisemblable le fait allégué* ».

Le commencement de preuve par écrit doit être complété par d'autres éléments dès lors qu'il ne s'agit pas d'une preuve parfaite.

Ces autres éléments de preuve sont généralement des témoignages, sous forme d'attestation écrite, ou encore un commencement d'exécution qui viendrait confirmer le fait allégué.

7.5 Actes en matière commerciale

Pour les actes entre commerçants, la preuve se fait librement (article 74 du Code de commerce), et il appartient au juge d'apprécier souverainement les éléments de preuve qui lui sont soumis.

Un écrit électronique simple, sans signature électronique, peut donc suffire à emporter la conviction du Juge. Le strict respect des exigences civilistes n'est ainsi pas déterminant.

Un problème se pose toutefois entre commerçants et non commerçants.

Dans l'hypothèse où un commerçant prend un engagement par e-mail envers un non commerçant, cette preuve pourrait lui être opposée mais pas l'inverse.

Cet écueil pourrait être contourné au moyen d'une convention sur la preuve (clause prévoyant dans le contrat que telle procédure vaudra preuve entre les parties).

En effet, une lecture à contrario de l'article 1163-2 du code civil laisse supposer que le législateur monégasque a souhaité donné existence aux conventions probatoires telles qu'elles existent en France depuis fort longtemps.

Les parties, qu'elles soient commerçantes ou non, pourraient donc convenir par exemple à l'avance que de simples e-mails, même non revêtus d'une signature électronique, seraient valables à titre de preuve. Le risque de clauses abusives a été soulevé par Me Giaccardi, d'autant qu'à ce jour aucune législation n'existe en la matière.

7.6 Vérification de la signature électronique

Si l'on accepte le principe de la signature électronique, il est cependant indispensable d'être vigilant quant à sa validation/vérification (voir à cet effet les références au règlement européen en préparation ci-après). En effet, pour être valable, encore faut-il que la signature soit conforme à certaines règles qui restent encore à définir au niveau des ordonnances souveraines mais qui néanmoins correspondent aux différents points suivants :

- **Aspect technique :** vérification de l'intégrité du contenu du document numérique ;
- **Aspect humain :** vérification de la force du lien entre le certificat électronique, lié à la signature, et la personne physique représentant le signataire. La force de ce lien dépend pour partie de la qualité de l'authentification de la personne, tant au moment de la délivrance du certificat qu'au moment de son utilisation. Pour une autre partie, la qualité de ce lien dépend de la confiance que l'on peut accorder à l'autorité de certification qui a délivrée le certificat et qui permet de s'assurer que les procédures prévues sont les bonnes et sont bien respectées ;
- **Aspect organisationnel :** vérification de la validité du certificat tant en matière de dates que de non révocation. Il s'agira également à ce niveau de vérifier la cohérence de l'usage effectif du certificat avec ce qui est prévu dans la Politique de Certification émise par l'AC.

La vérification d'une signature peut se faire à tout moment, mais si l'on souhaite pouvoir l'opérer dans le temps, encore faudra-t-il garder les éléments nécessaires à cette vérification sachant que de plus l'on ne maîtrise pas la pérennité de certaines AC. Par ailleurs, du simple fait de l'obsolescence cryptographique, devra-t-on mettre en place des dispositifs compliqués permettant de maintenir la qualité de la signature électronique dans le temps ?

7.7 Introduction à l'AGP (Autorité de Gestion de Preuve)

Afin de s'affranchir de l'ensemble de ces contraintes, il est également possible de s'appuyer sur le principe d'une AGP dont le rôle est de vérifier très en amont la signature électronique et d'émettre une attestation de preuve correspondant au résultat de la vérification.

La logique de l'AGP peut être internalisée en parallèle à un service d'archivage électronique mais il est préférable de l'externaliser dans une structure dédiée, fortement liée à l'état pour des raisons évidentes de légitimité mais surtout de pérennité. L'intérêt d'avoir recours à un tiers extérieur est qu'il aura en permanence la parfaite connaissance des différents formats de signature comme CADES, XADES ou encore PADES pour les plus connus, de même aura-t-il une bonne vision des formats spécifiques à certains pays et surtout le niveau de confiance à accorder à telle ou telle AC.

L'AGP est maintenant partie intégrante du dernier règlement européen : Article 34 du Règlement Européen N o 910/2014 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 23 juillet 2014.

8 RECOMMANDATIONS/PROPOSITIONS

De façon globale, le GTEN préconise que l'ensemble des transactions électroniques telles que présentées dans ce guide, puisse être encadré au plus tôt par les ordonnances souveraines afférentes à la loi 1.383 du 2 août 2011.

Par ailleurs et comme nous l'avons déjà signalé, il serait également opportun de travailler rapidement à la possibilité de supprimer les documents papiers après leur numérisation, afin de gagner à la fois en place et en efficacité d'accès à l'information.

Une autre proposition consiste pour la Principauté à s'intéresser de prêt à l'émergence d'une AGP (Autorité de Gestion de Preuve) destinée en premier lieu à valider les signatures électroniques et dont les services pourraient également s'étendre à une notion plus large de la preuve au sens numérique du terme.

En tant qu'Etat Souverain, l'émergence à Monaco de prestataires de services de confiance nationaux serait appréciable.

Enfin, il ne faut pas négliger la réflexion à mener concernant la mise en place de schémas d'identification appropriés aux besoins exprimés, sachant que le rôle de l'identité numérique en matière d'économie numérique est absolument primordial qu'il s'agisse d'un individu ou d'un document.

8.1 Comité du numérique

Par rapport à ce qui précède, on l'aura compris, il est indispensable de raisonner de façon transverse sur tous ces sujets. La cohérence sera ici le maître mot. De ce fait, nous proposons la création d'un comité du numérique avec comme base les membres du GTEN, auxquels pourraient venir se rattacher le Conseil Economique et Social, la Direction des Communications Electroniques, … Un tel comité pourrait également devenir par exemple une branche à part entière du Conseil Supérieur de l'Attractivité de la Principauté.

Un des rôles essentiels de ce comité serait en particulier de monter des actions de sensibilisation vis-à-vis du numérique pour tout type de populations en Principauté, à commencer par les établissements scolaires.

9 CONCLUSION

Même s'il s'est déjà écoulé plus de trois ans depuis la parution de la loi 1.383, cela devient finalement un avantage avec la parution du **règlement européen du 23 juillet** dernier, qui devrait permettre à la Principauté de proposer d'ores et déjà des services à la fois interopérables et surtout présentant un réel intérêt au niveau de l'Europe.

Par ailleurs, rappelons qu'en matière de développement autour du numérique, la Principauté dispose de réelles **opportunités**, en particulier en terme d'accès à des moyens de communication performants permettant de développer largement son attractivité.

De plus, **l'environnement est singulièrement favorable** compte tenu des attentes d'ores et déjà exprimées par les différents acteurs de la place, tant publics que privés, sans omettre l'aspect international et plus particulièrement la mise en œuvre du traité de Lisbonne du 13 décembre 2007 concernant les rapports de l'Union Européenne avec les *pays de petite dimension territoriale*. Monaco dispose ici d'une **formidable opportunité** de se positionner de façon significative et indépendante, comme un acteur important en matière du numérique par exemple en développant la notion d'AGP (Autorité de Gestion de Preuve) dont l'ensemble des pays européens et autres pourraient bénéficier, sachant que le règlement de juillet y fait déjà largement référence.

Quoiqu'il en soit et même si beaucoup reste à faire, des actions ont déjà été lancées. Aux niveaux légal et réglementaire, plusieurs chantiers sont en effet déjà ouverts concernant :

- l'économie numérique (attention à ce que sa mise en application ne soit pas bloquante),
- la cybercriminalité,
- les communications électroniques,
- l'adaptation du code pénal au numérique,
- la loi sur les données nominatives,
- le projet de loi sur les infractions informatiques.

Bien évidemment tous ces chantiers nécessitent une véritable cohérence. Il est absolument nécessaire de veiller à cette dernière au risque d'avoir de profondes et graves déconvenues.

Le comité du numérique, tel qu'évoqué au chapitre précédent, pourrait veiller à cette cohérence tout en recherchant des solutions transverse à la fois multi support et multi canal, afin d'offrir le plus de souplesse possible quant à leur utilisation mais aussi parfaitement **adaptées aux besoins** pour permettre leur très large diffusion, tant dans le domaine public que privé.

La version numérique du guide peut être téléchargée via l'URL : http://j.mp/gten2014 ou en scannant le QR Code suivant :